الفيروسات

وبرامج التجسس

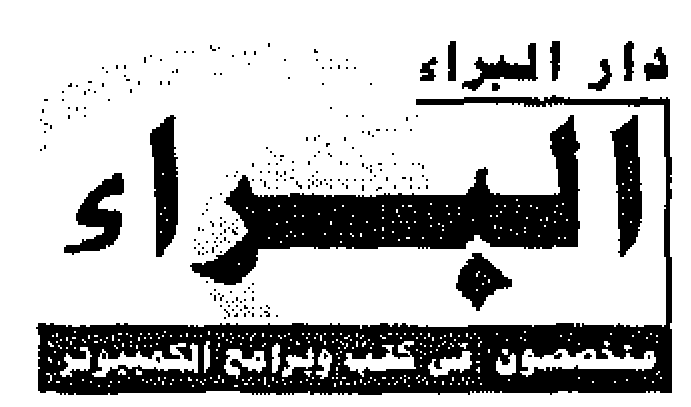
Viruses & Hacking



منحة 2005
SIDA
السويد

الفيروسات وبرامج التجسس

Computer Viruses And Hacking



المركز الرئيسي : 11 شارع د/محمد رأفت – محطة الرمل – الإسكندرية
تليفون وفاكس : 4838326 (03)(2+)
موبايل : 0101634294 (2+) - 0123357844 (2+)
Email : info@egyptbooks.net
URL : www.egyptbooks.net



وقل اعملوا فسيرى الله عملكم ورسوله والمؤمنون

صدق الله العظيم

حقوق النشر والطبع محفوظة 2005 ©

لا يجوز نشر أي جزء من هذا الكتاب أو إعادة طبعه أو اختزان مادته العلمية أو نقله بأي طريقة كانت اليكترونية أو ميكانيكية أو بالتصوير أو تسجيل محتوياته على اسطوانات مضغوطة (CD) سواء بصورة نصية أو بالصوت دون موافقة كتابية من الناشر ومن يخالف ذلك يعرض نفسه للمساءلة القانونية .

تحذير : الكتاب محمى بعلامات مميزة ومسجلة ومن يحاول التزوير يعرض نفسه ومعاونيه للمساءلة الجنائية .

طبعة يناير 2005

رقم الإيداع

2005/1907

ISBN

977-17-1966-1

مقدمة

لما لا نبدأ معا بداية غير تقليدية ...

لقد تناول العديد من الكتاب موضوع فيروسات الحاسب بأساليب متنوعة ومختلفة ..

فمنهم من قام بتشبيه الفيروس الذي يصيب الحاسب بالفيروس البيولوجي الذي يصيب الإنسان ، وحاول إيجاد وجه التشابه بين الاثنين ، وقام بعرض العديد من النظريات والمقارنات لتحديد أوجه الشبه والاختلاف بينهما ...

ومنهم من دخل في صلب الموضوع مباشرة وقام بحصر عدد كبير من فيروسات الحاسب المنتشرة وأوضح تأثيرها على الحاسب وكيفية علاجها ...

ومنهم من فلت زمام الأمور من بين يديه ، فراح يتحدث عن الفيروس على أساس أنه كائن أسطوري مبهم غير معروف الهوية ...

ومنهم من قام بتعقيد الأمور أكثر مما يجب ، فدخل في حوار لا أول له ولا آخر ، وذهب يخلط بين الفيروس وبين القرصنة ...

ولكل منهم – والحق يقال – أوجه تميز ، فأنا مثلكم في بداية تعاملي مع الحاسب ، لم أكن أعلم شيئا على الإطلاق حول موضوع الفيروس هذا .. وأدين بالفضل إلى الدكتور / خالد أبو الفتوح فضالة ، وهو من أوائل الكتاب العرب الذين تناولوا هذا الموضوع بشيء من التفصيل الذي أزاح الستار عن هذا الكائن غير معروف الهوية .

لذلك سوف اعقد معكم اتفاقا .. سوف نتفق على أنني لن أسلك أي من طرق الكتاب السابقين في تناول هذا الموضوع .. بل إنني سوف اعتبر نفسي أحد أصدقائكم الذي يملك الخبرة الكافية في هذا المجال ، ويرغب في نشر ما لديه من معلومات إليكم ...

تقولون ما الذي سوف أحصل عليه في المقابل ؟

بغض النظر عن الجانب المادي بالطبع – سوف أحصل على صداقتكم ، وهو أمر يسعدني كثيرا لو تعلمون ...

المؤلف

رامي عبد العزيز

blackrose157@yahoo.com

الفصل الأول

بداية لا بد منها

الفصل الأول

بداية لابد منها

أحب دائما أن أبدأ من نقطة الصفر ... هل تعلمون ما هي ؟
نقطة الصفر تتمثل في البيئة التي يصيبها الفيروس ثم يعمل من خلالها ويتكاثر ثم يبدأ في إصابتها بالعدوى .. ألا وهي وسائط التخزين ، أو إذا جاز تسميتها بالذاكرة .

فالذاكرة هي أي وحدة داخل الحاسب يمكن من خلالها تخزين البيانات سواء بشكل مؤقت أو دائم ، وسواء تتم عملية التخزين بواسطة المستخدم أو بواسطة الحاسب نفسه أو بواسطة الشركة المنتجة لمكونات الحاسب .

وبناء على ما تقدم ، فحتى يمكننا أن نتعرف على الفيروس ، لابد أولا أن نعرف ولو شيئا قليلا عن ماهية ذاكرة الحاسب وأنواعها .

أنواع الذاكرة :

يمكن تقسيم الذاكرة **Memory** بشكل أساسي إلى نوعين رئيسيين :

أولا- الذاكرة الداخلية :

وقد سمي هذا النوع باسم الذاكرة الداخلية **Internal memory** نظرا لأن المستخدم لا يقوم بالتعامل مع هذا النوع من أنواع الذاكرة بشكل

مباشر . حيث يقوم نظام التشغيل Operating system أو مصنعي أجزاء الحاسب بالتعامل بشكل مباشر مع هذا النوع .

وتنقسم الذاكرة الداخلية بدورها إلى نوعين :

1- ذاكرة القراءة فقط :

ويطلق عليها ROM اختصارا لـ (Read only memory) .

ولتوضيح وظيفة هذا النوع من الذاكرة أقرأ معي السطور التالية ..

من المعروف أن المعالج Processor الذي يمثل عقل الحاسب ويقوم بتنفيذ جميع الأوامر التي يصدرها المستخدم ، لا يعرف إلا لغة تسمى Machine language أو لغة الآلة ، وتتكون هذه اللغة من قيمتين هما (الصفر ، الواحد) .. !!!

ما هذا الذي تتحدث عنه ، كيف لا يفهم المعالج كل ما أطلبه منه وهو يقوم بتنفيذه سواء عرض أفلام أو ألعاب أو القيام بعمليات حسابية معقدة ، وتقول أنت أنه لا يفهم إلى قيمتين ؟

نعم ... صدقني فيما أقول .

عندما تقوم مثلا بالضغط على أحد الأفلام لعرضه ، فإنك بهذا تعطي أمرا للمعالج بعرض هذا الفيلم ، ومن ثم يقوم نظام التشغيل بإعادة صياغة الأمر الذي أصدرته للمعالج في صورة لغة الآلة ، وبالتالي يستطيع فهم وتنفيذ هذا الأمر.

والآن .. تخيل معي أنك قمت بتوصيل لوحة مفاتيح مثلا في المنفذ الخاص بها داخل اللوحة الأم ، فهل يستطيع المعالج التعرف على لوحة المفاتيح هذه وفهم ما الغرض من وجودها وكيفية عملها ؟

لا .. لا يستطيع المعالج من تلقاء نفسه التعرف على وظيفة هذه الوحدة الطرفية . ومن هنا تأتي أهمية ذاكرة القراءة فقط ROM .

فهذه الذاكرة تحتوى على مجموعة بيانات أساسية يتم كتابتها بواسطة الشركات المنتجة للوحة الأم ، وتحتوي على بيانات خاصة ببداية تشغيل الحاسب والتعرف على الوحدات الطرفية المتصلة به مثل لوحة المفاتيح أو الشاشة .. الخ

وبالتالي ، فإن المعالج بدون البيانات الموجودة داخل هذه الذاكرة لن يستطيع العمل إطلاقا ، لأنه ببساطة لن يستطيع التعرف على الوحدات المتصلة به ولا على كيفية عملها .

وفي فترة ليست ببعيدة ، قام أحد الطلاب الذين يدرسون هندسة الحاسب بتصميم فيروس أطلق عليه اسم تشيرنوبل ، وكانت وظيفة هذا الفيروس هو تخريب البيانات الموجودة داخل ذاكرة القراءة فقط ROM مما أدى إلى توقف ملايين أجهزة الحاسب حول العالم بالإضافة إلى الخسائر المادية الهائلة التي سببها هذا الفيروس .

إذا ، يمكن تلخيص ما سبق في أن وظيفة ذاكرة القراءة فقط هو أنها تحتوي على بعض البيانات الهامة المتعلقة بتعرف الحاسب على

الوحدات الطرفية المتصلة به وكيفيه عملها ، وبدون هـذه البيانـات سوف يتوقف الحاسب عن العمل تماما .

2- الذاكرة العشوائية :

النوع الثاني من أنواع الذاكرة الداخلية يطلق عليه الذاكرة العشـوائية RAM اختصارا لـ (Random Access Memory) .

ولفظة RAM منتشرة بكثرة بين المتعاملين مع الحاسب على الـرغم من أن العديد منهم لا يعلم الوظيفة الأساسية لهذا النوع من الذاكرة . فالذاكرة العشوائية الغرض منها هو العمل كوسـيط بـين وحـدات التخزين المختلفة والمعالج لسرعة وتنظـيم نقـل البيانـات وتنفيـذ الأوامر .

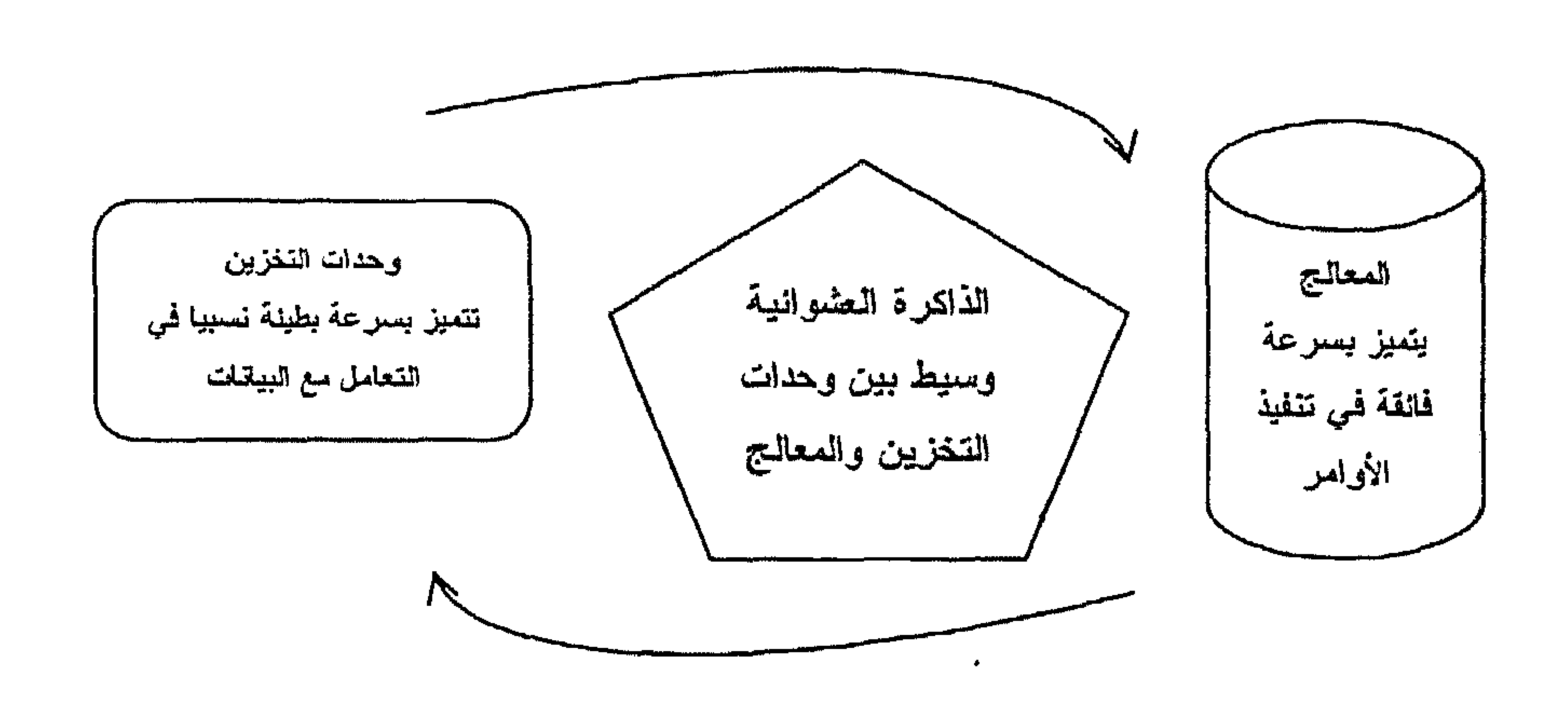
تخيل مثلا أنك ترغب في عرض فيلم موجود داخـل أحـد أجـزاء القرص الصلب **Hard Disk** ، فكل ما عليك القيام به هـو الضـغط مرتين بالمفتاح الأيسر للماوس فوق اسم هذا الفيلم ليبدأ عرضـه .. ولكن تخيل أن وراء هذا الأمر البسيط ملايين العمليـات الحسـابية المعقدة !!

فوحدات التخزين مثل **Hard Disk** سرعتها لا تعادل سـرعة تنفيـذ العمليات داخل المعالج ، ولو أنك انتظرت أن يتم تحميل جـزء مـن الفيلم إلى المعالج ليقوم بدوره بفك تشفير هذا الجزء تمهيدا لعرضه ،

فإن هذا سوف يعني أنك ستقضي وقتا طويلا منتظرا حتى يبدأ الحاسب في عرض هذا الجزء من الفيلم ..

ولكن الذي يحدث أن المعالج يقوم بنقل جزء من الفيلم إلى الذاكرة العشوائية ، ثم يقوم بمعالجة هذا الجزء وإرساله إلى الذاكرة العشوائية مرة أخرى ، ثم تقوم الذاكرة العشوائية بدورها بعرض هذا الجزء الذي تم فك تشفيره أمامك .. وهكذا حتى ينتهي الفيلم .

ويمكن توضيح هذه العمليات من خلال الشكل التوضيحي التالي :



ثانيا- الذاكرة الخارجية :

الذاكرة الخارجية **External Memory** تتمثل في وسائط التخزين المختلفة التي يتعامل معها المستخدم بشكل مباشرة مثل **Hard Disk** أو **Floppy Disk** أو **CD** .

والذاكرة الخارجية بأنواعها من أكثر وسائل نشر الفيروس بين المستخدمين عن طريق عملية تبادل البيانات المصابة بالفيروس باستخدام هذه الوسائط .

أنواع البيانات التي يصيبها الفيروس :

يحتاج الفيروس دائما إلى عائل يساعده على البقاء والانتشار حتى يبدأ بالتكاثر وإصابة الحاسب بالأضرار المصمم من أجلها .

وهذا العائل يتمثل في ثلاث أنواع رئيسية من الملفات التي تستخدم دائما داخل التطبيقات المختلفة ، وهي :

1. **الملفات التنفيذية** : ويطلق عليها اسم **Executable files** وهي الملفات التي تحمل الامتداد **EXE** .
2. **ملفات الأوامر** : ويطلق عليها اسم **Command files** وهي الملفات التي تحمل الامتداد **COM** .
3. **ملفات حزم الأوامر** : ويطلق عليها اسم **Batch files** وهي الملفات التي تحمل الامتداد **BAT** .

ما المقصود بالامتداد ؟

الامتداد **Extension** هو عبارة عن رمز يتكون عادة من ثلاثة حروف توجد في نهاية اسم الملف .. فإذا كنت مثلا من المتعاملين مع برنامج **Microsoft Word** سوف تلاحظ أن كل الملفات التي تقوم بحفظها أو التعامل معها تحمل الامتداد **DOC** .

والغرض من وجود هذا الرمز هو تحديد نوعية البرامج التي يمكنها تشغيل ملف معين .. فمثلا عند الضغط على أي ملف تم حفظه بواسطة برنامج **Word** ، سوف تلاحظ أن نظام التشغيل سيقوم مباشرة بتشغيل برنامج **Word** وعرض الملف من خلاله .

وهذا ليس سحرا ، فكل ما هنالك أن نظام التشغيل يحتوي على قاعدة بيانات عن البرامج المثبتة على الحاسب ونوعية الملفات التي تتعامل معها ، فعند الضغط على أي ملف ، يقوم نظام التشغيل بقراءة امتداد الملف ، ومن ثم تحديد البرنامج المناسب لعرض هذا الملف .

وبالتالي فإنك عندما تقوم بالضغط على ملف يحتوي على فيلم ، فإن نظام التشغيل يقوم بتشغيل برنامج **Media player** مثلا لتتمكن من مشاهدة الفيلم .

وبالمثل إذا لم يوجد برنامج مناسب لعرض الملف فإن نظام التشغيل سوف يظهر لك رسالة تفيد بأنه لا يستطيع تحديد نوعية البرنامج المناسب لعرض هذا الملف ، ثم يقوم بعرض نافذة تحتوي على جميع البرامج المثبتة على الحاسب لتختار منها البرنامج المناسب لتشغيل الملف، وينتج ذلك عادة عن وجود خطأ في قاعدة بيانات نظام التشغيل التي يطلق عليها اسم **Registry**.

ويمكنك استعراض هذه القاعدة عن طريق كتابة كلمة **regedit** داخل النافذة **Run** ثم الضغط على مفتاح **Ok** .. ولكن يجب توخي الحظر وعدم تغيير أي بيانات داخل هذه القاعدة حتى لا يحدث خلل داخل النظام .

والآن نعود لموضوعنا عن العائل الذي يحتاجه الفيروس للانتشار .

فالنوع الأول من الملفات يسمى بالملفات التنفيذية ، وهي عبارة عن ملفات تحمل الامتداد EXE يتم كتابتها بواسطة لغة الآلة وتكون غير مفهومة إلا بالنسبة للمتخصصين في هذه اللغة .



ولكن ، ما هو الغرض من وجود هذه الملفات ؟ وما هي وظيفتها ؟

عندما تحاول تشغيل لعبة معينة داخل الحاسب ، سوف تلاحظ أن المجلد الخاص بتلك اللعبة يحتوي على العديد من الملفات التي قد تصل إلى آلاف الملفات في بعض الأحيان .. ولكنك سوف تلاحظ أيضا أن هناك ملف واحد فقط عند الضغط عليه يتم تشغيل اللعبة ، وهذا هو الملف التنفيذي الذي يقوم بتشغيلها أو تشغيل أي برنامج آخر ، وبدون وجوده لن تستطيع تشغيل أي برنامج على الحاسب .

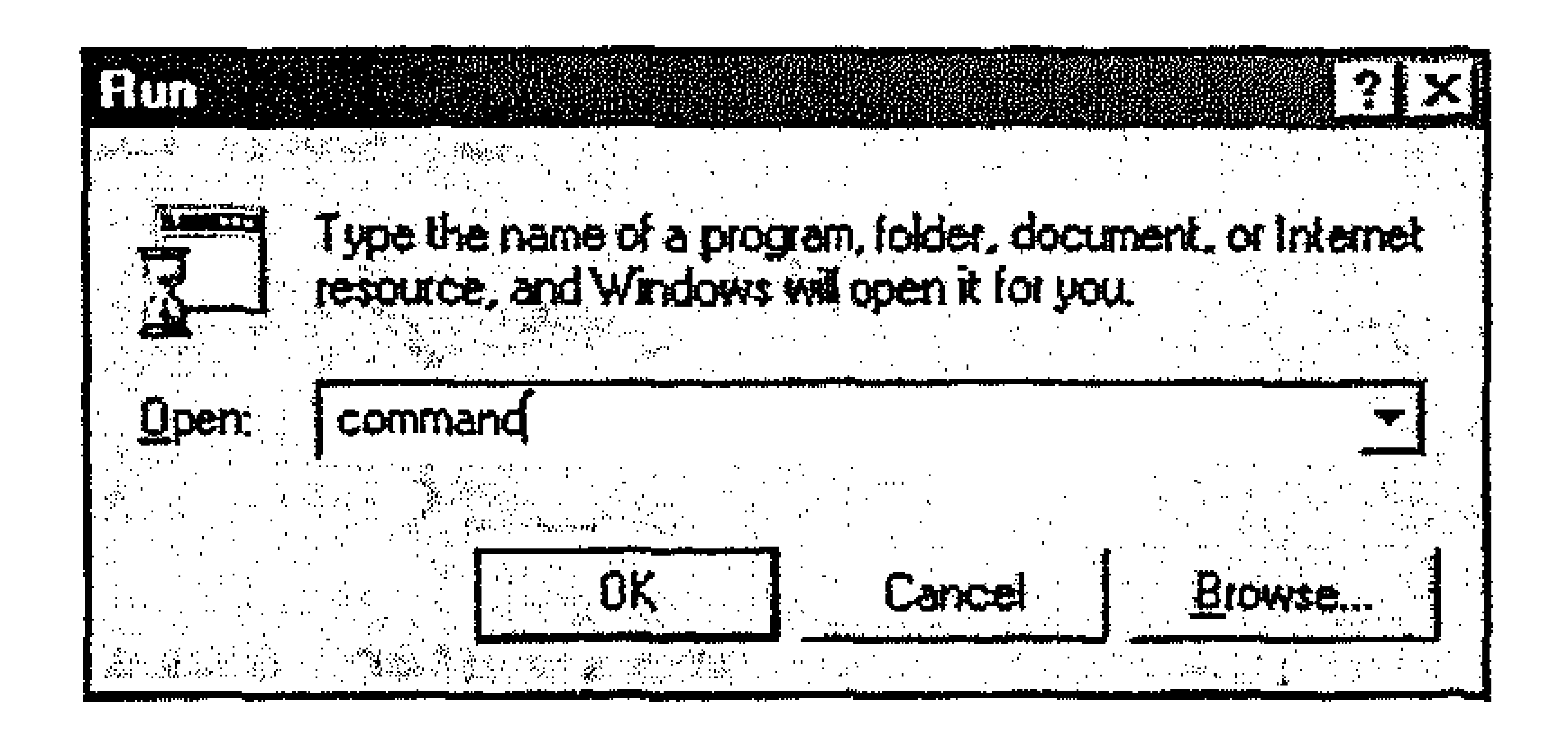
وبالمثل فإن النوع الثاني من الملفات الذي يطلق عليه ملفات الأوامر يشبه الملفات التنفيذية من حيث الوظيفة والغرض ، ويكتب أيضا باستخدام لغة الآلة .

أما النوع الثالث من الملفات فيسمى ملفات حزم الأوامر **Batch files** وهذه النوعية من الملفات تحتوي على مجموعة من أوامر **DOS** تقوم بوظيفة معينة داخل الحاسب .. وتستخدم هذه الملفات في تصميم بعض البرامج التي كانت تعمل داخل نظام تشغيل **DOS** قبل ظهور أنظمة التشغيل الحالية .

وإنشاء هذه الملفات لا يحتاج إلى خبرة في إحدى لغات البرمجة ، فكل ما تحتاجه هو معرفة بأوامر **DOS** .

ومثلا على كيفية إنشاء هذا النوع من الملفات ، اتبع الخطوات التالية :

1. من القائمة **Start** ، اختر العنصر **Run** ، ثم اكتب كلمة **Command** لتحميل نظام تشغيل **Dos** داخل بيئة عمل **Windows** كما في الشكل التالي :



2. سوف يتم تحميل نظام تشغيل **Dos** ، فقم بالضغط على مفتاحي **ALT + Enter** لتكبير الصورة ، ثم أدخل الأمر التالي :

C:\Windows\Desktop> CD\

ثم اضغط مفتاح **Enter** كما في الشكل التالي :

```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS\Desktop>cd\
```

3. قم بكتابة الأمر التالي لإنشاء ملف باسم **Ramy** يحمل الامتداد **BAT** :

C:\> edit Ramy.bat

فتظهر نافذة برنامج **Edit** وهو أحد البرامج التي كانت تستخدم في كتابة وتنسيق البيانات داخل نظام **DOS** ، كما في الشكل التالي :

```
 File  Edit  Search  View  Options  Help
                          C:\ramy.bat
cls
@ECHO [HI THIS IS A DEMO]
@ECHO OFF
```

4. قم بكتابة الأوامر داخل برنامج **Edit** كما تظهر في الشكل السابق ، ثم من خلال القائمة **File** ، أحفظ الملف ، ثم أخرج من البرنامج للعودة مرة أخرى إلي نظام **DOS** .

5. قم بتشغيل الملف الذي تم إنشائه عن طريق كتابة اسم هذا الملف ، ثم اضغط مفتاح **Enter** ، كما في الشكل التالي :

```
[HI THIS IS A DEMO]
C:\>_
```

ويجب ملاحظة أن هذا النوع من الملفات لا يستخدم الآن نظرا لانتشار أنظمة تشغيل **Windows** بإصداراتها المختلفة .



وهنا يثار تساؤل هام .. ما علاقة هذه الملفات بالفيروس ولماذا يعتمد عليها الفيروس كعائل للانتشار داخل الحاسب ؟

والإجابة بسيطة ، فالأنواع الثلاثة السابقة هي أكثر الملفات استخداما عند التعامل مع التطبيقات المختلفة ..

فعندما تقوم بتشغيل أي تطبيق أو برنامج فإنك سوف تحتاج إلى استدعاء الملف التنفيذي الخاص بهذا التطبيق ، وهذا يعني أنه لو استطاع الفيروس أن يقوم بكتابة نفسه داخل ملف تنفيذي واحد على الحاسب ، فإنه في كل مرة يتم فيها تشغيل هذا البرنامج ، فإن الفيروس سوف يقوم بنشر نفسه داخل ملف أو مجموعة ملفات أخرى مما يضمن له البقاء لحين ظهور آثاره التخريبية .



هل يقوم الفيروس بإصابة الأنواع السابقة فقط من الملفات ، أم أنه يصيب جميع الملفات الموجودة داخل الحاسب ؟

يمر الفيروس بعدة مراحل أثناء إصابة الحاسب كما يحدث بالنسبة للفيروس البيولوجي الذي يصيب الإنسان .

ففي البداية كل ما يحتاجه الفيروس هو الانتشار ، ولذلك فإن الفيروس يقوم بالتركيز على الملفات التنفيذية فقط . أما بعد الانتهاء من المرحلة الأولي ، فإن هناك بعض الفيروسات التي تكتفي فقط بإصابة الملفات التنفيذية – وهو النوع الشائع من الفيروسات – وهناك البعض الآخر الذي يقوم بإصابة أنواع الأخرى من الملفات مثل ملفات المكتبات الموجودة داخل نظام **Windows** والتي تحمل الامتداد **DLL** .



لماذا لا يقوم الفيروس بإصابة ملفات الأفلام والأغاني ؟

لقد تعرضت إلى أنواع أكثر مما تتخيلها من الفيروسات المختلفة ، ولكني لم أجد نوع واحد من هذه الفيروسات يستطيع إصابة ملفات الأغاني أو الأفلام .. وهو أمر محير بالفعل !!

ولكني اعتقد أن الإجابة تكمن في النقاط التالية ..

1. عادة ما تكون هذه الملفات حجمها كبير جدا ، وذلك بعكس الملفات التنفيذية التي تتميز بصغر الحجم ، وهذا يعني أن الفيروس يمكنه إصابتها بسهولة .
2. عندما يصيب الفيروس الملف التنفيذي فإنه عادة ما يتسبب في تخريب هذا الملف ، أو أنه يكتفي فقط بنسخ نفسه في نهاية الملف التنفيذي بحيث يضمن أنه في كل مرة يتم فيها تشغيل هذا الملف سوف ينتشر الفيروس .. أما بالنسبة لملفات الأفلام أو الأغاني فإنها تكون على درجة عالية من التشفير وأي تغيير سواء بالحذف أو الإضافة داخل هذه الملفات سوف يؤدي إلى تخريبها ، مما يعني أن الفيروس سوف يكشف عن نفسه مبكرا قبل الانتهاء من مرحلة الانتشار التي يحتاجها في بداية إصابة الحاسب .

3. عندما يقوم أحد الأشخاص بتصميم فيروس ، فإن أقصى ما ينشده من وراء ذلك هو الانتشار وإحداث أكبر آثار تخريبية ممكنة ، وبالتالي فإنه يعتمد على تخريب الملفات التنفيذية التي يتعامل معها أي مستخدم للحاسب سواء داخل الشركات أو الهيئات المختلفة أو بالنسبة للمستخدم العادي .. أما إذا اعتمد الفيروس على إصابة ملفات الأغاني والأفلام ، فإنه بذلك سوف يقلص من احتمال إصابة أكبر عدد ممكن من الأجهزة ، حيث أنه بالنسبة للشركات والمكاتب لا يسمح بتداول مثل هذه الأنواع من الملفات .

الفصل الثانى

الفيروس

الفصل الثاني

الفيروس



ما هو الفيروس ؟

عندما يُطرح هذا السؤال .. عادة ما سوف تسمع آراء أغرب من الخيال .. بل أغرب من الأساطير اليونانية نفسها !!

لا تقلق .. إنه ليس نوع من أنواع البكتريا التي تصيب الحاسب أو وباء ينتشر في الجو ويصيب الأجهزة ..

لما لا تنسى كل ذلك ونحاول معا وضع تعريف بسيط ومنطقي لفيروس الحاسب ..

1. هو عبارة عن برنامج يحتوي على مجموعة من الأوامر .
2. يتم كتابة هذا البرنامج باستخدام إحدى لغات البرمجة منخفضة المستوى .
3. يصيب الحاسب عن طريق نقل الملفات المصابة بالفيروس .
4. له آثار تخريبية .

هل وجدت من قبل تعريف أبسط من هذا ؟

والآن لما لا نتعرف على كل نقطة من النقاط السابقة بشيء من التفصيل .

1. الفيروس عبارة عن برنامج :

نعم .. الفيروس ما هو إلا عبارة عن برنامج مثل أي برنامج آخر . فأنت لا تحتاج إذا إلى ارتداء قفازات واقية حتى لا تنتقل إليك العدوى التي تصيب الحاسب .

وهذا البرنامج يحتوي على عدد من الأوامر الخاصة بكيفية انتشاره داخل الملفات وتكرار نفسه والآثار التخريبية الخاصة به .

2. يكتب باستخدام إحدى لغات البرمجة منخفضة المستوى :

من يقومون بالتعامل مع لغات البرمجة ، يعرفون جيدا أنه عادة ما يتم تقسيم لغات البرمجة إلى نوعين أساسيين .

- **لغات البرمجة مرتفعة المستوى :**

ويطلق عليها **high level language** وتتمثل عادة في لغات البرمجة التي تعمل تحت بيئة **Windows** بمختلف إصداراتها .. حيث تحتاج هذه اللغات إلى وجود مترجم **Compiler** يعمل كوسيط بين الأوامر الخاصة بهذه اللغات وبين المعالج .. أي أنه يمكن تعريف اللغات عالية المستوي بأنها اللغات التي لا تتعامل مباشرة مع لغة الآلة وإنما

تحتاج دائما إلى مترجم بينها وبين المعالج . ومن أمثلة هذه اللغات **Visual Basic** ، **C** ، **Java** .

- **لغات البرمجة منخفضة المستوى** :

ويطلق عليها **Low level language** ، وهي اللغات التي تتعامل مباشرة مع لغة الآلة ، ومن أمثلتها **Assembly language** أو كما يسميها البعض لغة التجميع .. وتعتبر هذه اللغة من اللغات المندثرة نظرا لصعوبة استخدامها ، وعادة ما تستخدم بواسطة من يدرسون هندسة الحاسب .

وعادة ما يكتب الفيروس بواسطة إحدى لغات البرمجة منخفضة المستوى ، والسبب في ذلك أن هذه اللغات تضمن أن يكون ملف الفيروس صغير الحجم للغاية مما يعني قدرة أكبر على التخفي داخل الحاسب .

بالإضافة إلى أن لغات البرمجة المنخفضة يمكن من خلالها تصميم برامج مستقلة تعمل بمفردها دون الحاجة إلى ملفات مساعدة للبرنامج ، ويطلق على هذا النوع من الملفات **Stand alone programs** ، أي أن الناتج النهائي للبرنامج يكون في شكل ملف واحد فقط .

وهذا بالضبط ما يحتاجه الفيروس ، فلو أنك على علم بإحدى لغات البرمجة مرتفعة المستوي ، فأنت تعلم أن البرامج التي تصمم بواسطة هذه اللغات لا يمكنها العمل بمفردها ، بل تحتاج إلى أن تقوم بإنشاء

حزمة **Package** تحتوي على مجموعة من الملفات المساعدة للبرنامج ثم يتم دمج هذه النسخة مع ملف يطلق عليه **Setup** حتى يتمكن المستخدم من تثبيت البرنامج على الحاسب .. وهذا أمر لا يتصور حدوثه مع الفيروس .

فمن غير المعقول أن تقوم بتصميم فيروس يحتاج إلى أن يقوم المستخدم بتثبيته على الحاسب حتى يبدأ بالعمل !!!

3. الفيروس يصيب الحاسب عن طريق نقل الملفات المصابة:

من أكثر الأساليب الشائعة في إصابة الفيروس للحاسب أن تقوم بنقل بعض البيانات أو الملفات المصابة بالفيروس إلى حاسبك الشخصي ، ومن أكثر أنواع الملفات التي تصاب بالفيروس هي الألعاب ، وذلك نظرا لانتشارها وتداولها الكبير بين مستخدمي الحاسب .

إذا ، يمكن القول أن العامل الأول لنشر الفيروس هو تداول البيانات الموجودة داخل وحدات التخزين المصابة بالفيروس .

ولكن هذا لا يعني أنه لا يوجد وسائل أخرى لنشر الفيروس ؛ بل إن هناك عامل آخر فعال جدا ، وهو تداول البيانات الموجودة داخل شبكة الإنترنت .. فمن الممكن أن يقوم مصمم الفيروس بزرعه داخل رسالة ثم إرسالها إلى أكبر عدد ممكن من المستخدمين بشكل عشوائي .. وسوف نتعرض لهذا النوع من الفيروسات في جزء لاحق من الكتاب.

4. الآثار التخريبية للفيروس :

الآثار التخريبية للفيروس متنوعة وكثيرة ، فمنها ما يقوم بحذف البيانات الموجودة داخل الحاسب ، ومنها ما يقوم بإبطاء الحاسب ، ومنها ما يقوم باستغلال الذاكرة العشوائية بحيث لا يمكن تشغيل أي برنامج ، ومنها أيضا ما يصمم لأغراض استعراضية ترضي غرور مصمم الفيروس دون أن تضر بالحاسب ، ومنها ما يكتب لأغراض التجسس .. وهو ما يطلق عليه **Spay Ware** .

الفصل الثالث

مراحل الإصابة

الفصل الثالث

مراحل الإصابة

عندما يبدأ الفيروس في إصابة الحاسب ، فإن عملية الإصـــابة تمــر بعدة مراحل يختلف مدى تحققها باختلاف نوع الفيروس .
ولذلك ؛ فإننا سوف نخصص هذا الفصل للحديث بشيء من التفصيل عن هذه المراحل ومدى أهميتها .

1. المرحلة الأولي : الإصابة

تتمثل أولي مراحل إصابة الفيروس للحاسب في أن يقوم المســتخدم بتشغيل الفيروس على الحاسب ليصيب على الأقل ملف واحد فقــط ، وتتم هذه العملية عن طريق نقل بعض البيانات المصابة بـــالفيروس إلى الحاسب ، وذلك إما عن طريق تداول البيانات بواسطة وحــدات التخزين المختلفة ، أو عن طريق الحصول علـــى بعــض البيانـــات المصابة بالفيروس من خلال شبكة الإنترنت .



وهنا يثور تساؤل هام .. إذا كان أحد أصدقائي يمتلك بعض البيانات المخزنة على القرص الصلب **Hard Disk** الخاص به

مع العلم أن هذا القرص الصلب مصاب بنوع من الفيروس ، وأرغب في الحصول على هذه البيانات بالرغم من أن الحاسب الخاص بي لا يحتوي على برنامج مضاد للفيروسات .. فهل أستطيع أن أغامر وأحصل على هذه البيانات ؟ وفي هذه الحالة ، هل سينتقل الفيروس إلى أم لا ؟

الإجابة على هذا التساؤل تنقسم إلى شقين ..

الشق الأول : يتمثل في طبيعة البيانات التي ترغب في نقلها ، فإذا كانت هذه البيانات عبارة عن أفلام أو أغاني ، ففي هذه الحالة يمكنك أن تقوم بنقل هذه البيانات إلى الحاسب الخاص بك ، وتكون نسبة الإصابة في هذه الحالة 50% . أما بالنسبة لـ 50% الباقية فتعتمد على نوع الفيروس الموجود بالقرص الصلب .

أما إذا كانت البيانات التي ترغب في الحصول عليها هي عبارة عن برامج تحتوي على ملفات تنفيذية . فلا تغامر مطلقا بالقيام بهذه المهمة.

الشق الثاني : فيتمثل في نوع الفيروس الموجود على القرص الصلب . فإذا كان هذا الفيروس يقوم بإصابة الملفات التنفيذية – التي تحدثنا عنها سابقا – فلا يوجد هناك ضرر من نقل البيانات إذا كانت لا تحتوي على

ملفات تنفيذية – مثل الأفلام أو الأغاني – أما إذا كان الفيروس لا يصيب الملفات التنفيذية مثل فيروس Worm stator الذي يقوم بإنشاء ملفين داخل كل مجلد موجود على القرص الصلب ، فإنه في هذه الحالة لا ينبغي الحصول على أي بيانات مطلقا ، لأن إصابة حاسبك بهذا الفيروس سوف تكون أكيدة .

2. المرحلة الثانية : الكمون والانتشار

المرحلة الثانية في العدوى تتمثل في مرحلة الكمون والانتشار ، وهي مرحلة اختيارية تختلف بطبيعتها حسب نوع الفيروس .

فهناك بعض الفيروسات التي تقوم بإظهار آثارها التخريبية بمجرد إصابة الحاسب مباشرة . وعادة ما يمكن احتواء الآثار التخريبية لهذا النوع من الفيروسات بسهولة لأنها تقوم بالكشف عن نفسها خلال فترة مبكرة من الإصابة ، فلا تكون أضرارها كبيرة .

وهناك نوع آخر من الفيروسات الذي يتميز بفترة حضانة كبيرة تتراوح ما بين شهر إلى عدة أشهر ، وخلال هذه الفترة الكبيرة لا يظهر الفيروس أي أعراض على الحاسب المصاب ، بل يكتفي بالانتشار وإصابة أكبر عدد ممكن من الملفات . وذلك يضمن لهذا

النوع من الفيروسات الانتشار بين أكبر عدد ممكن من المستخدمين ، لأن المستخدم لا يشعر بوجود أي شيء غير مألوف على الحاسب .
وعادة ما تكون الآثار التخريبية لهذا النوع من الفيروسات جسيمة ، كما يحتاج هذا النوع من الفيروسات إلى مجهود كبير حتى يمكن التخلص منه .. وسوف تكون محظوظا إذا تمكنت من إزالة هذا الفيروس دون حدوث خسائر .
إذا ، يمكن القول أن مرحلة الكمون والانتشار هي مرحلة اختيارية يتوقف حدوثها على نوع الفيروس .

3. المرحلة الثالثة : إعلان الفيروس عن نفسه

ويطلق البعض على هذه المرحلة اسم جذب الزناد ، حيث يقوم الفيروس خلال هذه المرحلة بالإعلان عن وجوده . وعادة ما تكون هذه المرحلة قصيرة للغاية ، وتسبق مباشرة المرحلة الأخيرة .
وهناك عدة طرق يستخدمها الفيروس في الإعلان عن نفسه وفقا لنوعه يمكن حصرها في النقاط التالية :

1. بطء في التعامل مع الحاسب ، ويزيد هذا البطء كلما طالت المدة .
2. عدم القدرة على تشغيل بعض البرامج والتطبيقات ، وتزيد عدد التطبيقات الغير قادرة على العمل كلما زادت الفترة .

وعادة ما يقوم نظام التشغيل بإظهار رسالة بالشكل التالي كلما حاولت تشغيل أحد التطبيقات المصابة :

This Program has performed illegal operation and will shutdown .

3. اختفاء بعض الملفات تدريجيا .
4. ظهور بعض الملفات بشكل تدريجي ، وعادة ما تكون هـذه الملفات من نوع **Hidden** ، وتزداد هـذه الملفـات بشـكل ملحوظ مما يؤدي إلى تآكل المساحة التخزينية الموجودة على القرص الصلب .
5. ظهور رسائل خطأ كثيرة ومتنوعة بالرغم من عـدم وجـود سبب منطقي لظهورها .
6. ظهور رسائل غريبة يقوم فيها الفيروس بالإعلان عن نفسه ، ويطلق على هـذا النـوع مـن الفيروسـات بالفيروسـات الاستعراضية . وعادة ما نلاحظ أن من يقوم بتصـميم هـذا النوع من الفيروسات كل ما يحتاجه هو الشهرة ، فهو يكتفي فقط باستعراض قدراته في تصميم البرامج فقط دون الاهتمام بإحداث آثار تخريبية على الحاسب .

4. المرحلة الرابعة : الاجتياح

أما بالنسبة للمرحلة الرابعة والأخيرة ، فهي مرحلة الاجتياح وإظهار الآثار التخريبية . وتختلف أيضا الآثار التخريبية وفقا لنوع الفيروس

الذي يصيب الحاسب ، ويمكن حصر هذه الآثار في النقاط التالية ترتيبا من الأقل ضررا إلى الأكثر :

1. بطئ شديد في الحاسب مما يجعل التعامل معه مستحيلا .
2. عدم القدرة على تشغيل معظم التطبيقات ، وكلما حاولت تشغيلها تظهر رسائل خطأ .
3. مسح الملفات التنفيذية للبرامج ، سواء المثبتة داخل نظام التشغيل أو Source التي تحتفظ بها داخل الحاسب . وهذا يعني عدم القدرة على تشغيل هذه التطبيقات في كلتا الحالتين .
4. حذف ملفات FAT مما يعني حذف جميع البيانات الموجودة داخل القرص الصلب .. وهو الأمر الأكثر خطورة .
5. إصابة أحد أجزاء المكونات الصلبة مثل فيروس تشيرنوبل الذي يقوم بإصابة نظام الإدخال والإخراج الأساسي BIOS مما يؤدي إلى توقف الحاسب بالكامل ، وتحتاج في هذه الحالة إلى إعادة برمجة هذه الشريحة مرة أخرى عن طريق متخصص .. وعادة ما يكون هذا النوع من الفيروسات نادر جدا .

لفظ FAT يتردد كثيرا لكني لا أعرف ماذا يعني ؟
هذا اللفظ اختصار لـ File Allocation Table ، وهو لفظ يعرفه المتعاملين في صيانة الحاسب . فمن المعروف أن القرص الصلب Hard Disk يتكون في الداخل من مجموعة من الأسطوانات تشبه CD ، وتقوم مجموعة من الإبر بالدوران فوق هذه

الأسطوانات لكتابة وقراءة البيانات المخزنة .
والآن تخيل معي أنك قمت بتشغيل برنامج **My Computer** ثم قمت باختيار أحد أجزاء القرص الصلب ، واستعرض البيانات الموجودة داخل مجلد مخزن على هذا الجزء .. هذه العملية البسيطة التي تقوم بها مرارا ورائها عدد من العمليات المعقدة التي لا تتخيلها .
فكيف تعرف رؤوس القراءة والكتابة الموجودة داخل القرص الصلب أماكن تخزين هذه البيانات .. إذا الأمر يحتاج إلى دليل
وهذا هو وظيفة ملفات **FAT** ، فهي عبارة عن ملفات يتم تخزينها داخل القرص الصلب مباشرة ، ولا يمكن للمستخدم العادي التعامل معها بشكل مباشر إلا عن طريق لغة الآلة . وتحتوي هذه الملفات على فهرس بأماكن تخزين كل ملف ومجلد على القرص الصلب ، وتستخدم رؤوس القراءة والكتابة هذا الفهرس لضمان سرعة الوصول إلى البيانات .
والآن ، تخيل أن الفيروس أصاب هذه الملفات .. فكيف يمكن لرؤوس القراءة والكتابة الوصول إلى أماكن تخزين المعلومات داخل القرص الصلب ..
إذا ما يحدث في الواقع أن الفيروس لا يقوم بحذف البيانات فعليا من داخل القرص الصلب ، وإنما يكتفي بمسح الفهارس المخزن بها أماكن وجود هذه البيانات ، فيظهر القرص الصلب وكأنه خالي تماما .
ولذلك ، قامت شركة **Symantec** التي تقوم بإنتاج مجموعة برامج **Norton** بإنشاء برنامج أطلقت عليه اسم **Rescue** ، وهو عبارة عن ملف صغير للغاية يأتي ضمن برنامج **Norton Anti Virus** ، ووظيفة هذا البرنامج الصغير هو أخذ نسخة من ملفات **FAT** وحفظها على **Floppy Disk** بحيث يمكن استعادتها مرة أخرى في حالة إصابتها بالفيروس .

الفصل الرابع

أنواع الفيروسات

الفصل الرابع
أنواع الفيروسات

إذا حاولت القيام بحصر الفيروسات المنتشرة ، فإنك بالتأكيد سوف تفشل في ذلك نظر للكم الهائل من الفيروسات المنتشرة حول العالم . ولكن على أية حال ، يمكن القيام بتصنيف الفيروسات داخل مجموعات تتشابه من عدة أوجه كما يلي :

1- فيروسات الكتابة :

وهذه المجموعة من الفيروسات تتشابه من حيث المكان الذي يصيبه الفيروس داخل الحاسب . وتنقسم هذه المجموعة إلى قسمين كالتالي :

القسم الأول :

ويتمثل في الفيروسات التي تصيب الملفات التنفيذية الموجودة داخل الحاسب أو ملفات الأوامر . حيث يقوم هذا النوع من الفيروسات بنسخ نفسه داخل الملفات التنفيذية ، وهنا نجد أن برنامج الفيروس يقوم بإصابة الملفات التنفيذية بإحدى طريقتين ..

الأولي : أن يقوم الفيروس بنسخ نفسه في بداية الملف التنفيذي ، وهذا يعني أن الأوامر الموجودة في بداية الملف التنفيذي سوف يتم استبدالها بأوامر الفيروس . مما يعني أن الفيروس

بمجرد أن يصيب الملف التنفيذي سوف يؤدي إلى إحداث خلل به .

ويطلق على هذا النوع من الفيروسات اسم فيروسات الكتابة الفوقية **Over writing viruses** نظرا لأن الفيروس يقوم باستبدال الجزء الأول من الملف التنفيذي .

وعادة ما تظهر أعراض الإصابة بهذا النوع من الفيروسات بشكل مباشر وفوري ، حيث أن هذا النوع لا يحتاج إلى فترة كمون ، وبالتالي يمكن السيطرة عليه بمجرد ظهور أعراض الإصابة .

الثاني : أما النوع الثاني من طرق إصابة الملفات التنفيذية ، فيتمثل في أن يقوم برنامج الفيروس بنسخ نفسه في نهائية الملف التنفيذي ، وهذا يعني أنه لن يقوم بحذف أي جزء من الملف التنفيذي ، بل سوف يكتفي الفيروس بأن يستخدم الملف التنفيذي كعائل يتم من خلاله استدعاء الفيروس ليقوم بتكرار نفسه وإصابة أكبر عدد ممكن من الملفات قبل أن تظهر أعراض الإصابة .

ويطلق على هذا النوع اسم فيروسات الكتابة غير الفوقية **Non Over writing viruses** . وبالطبع يتميز هذا النوع بفترة كمون طويلة قبل أن تظهر أعراض الإصابة ، حيث

يستغل الفيروس هذه الفترة في إصابة أكبر عدد ممكن من الملفات قبل الإعلان عن نفسه .

وعادة ما يكون هذا النوع أشد خطورة من النوع السابق ، لأن فترة الكمون تؤدي إلى إصابة عدد كبير من الملفات ، وبالتالي فإن عملية التخلص من الفيروس تكون شاقة وتحتاج إلى مجهود كبير .

القسم الثاني :

وبالنسبة للقسم الثاني من فيروسات الكتابة ، فتتمثل في الفيروسات التي تقوم بنسخ نفسها داخل ملف خفي **Hidden File** على أحد وحدات التخزين . وبالطبع يمكن اكتشاف هذا النوع بسهولة إذا كانت لديك الخبرة الكافية لاكتشاف الملفات الخفية الغريبة عن ملفات نظام التشغيل.

كما يوجد نوع آخر من الفيروسات الذي يقوم بنسخ نفسه على الأسطوانة مباشرة دون أن يحتاج إلى ملف . حيث يقوم الفيروس بكتابة نفسه داخل الاسطوانة الصلبة مباشرة باستخدام لغة الآلة ، ثم يقوم بكتابة برنامج فرعي آخر داخل منطقة يطلق عليها اسم **Boot Record** – وهي المنطقة التي تحتوي على بيانات نظام التشغيل التي يستخدمها الحاسب لقراءة تعليمات النظام عند بدأ

العمل - ، ويستخدم هذا البرنامج الفرعي لاستدعاء برنامج الفيروس في كل مرة يتم فيها تشغيل الحاسب .

وهذا النوع من الفيروسات كان يتميز بصعوبة بالغة في اكتشافه فيما مضى ، أما الآن فيمكن اكتشافه بسهولة ، حيث قامت الشركات المصنعة للوحة الأم بتعديل برامج التشغيل الأساسية للحاسب المخزنة على شريحة **BIOS** عن طريق تطوير برنامج التشغيل وإضافة برنامج مضاد للفيروسات .

وهذا البرنامج في حقيقة الأمر لا يستطيع التعرف على جميع أنواع الفيروسات ، بل إنه مصمم فقط لاكتشاف الفيروسات التي تحاول أن تقوم بكتابة نفسها مباشرة داخل منطقة **Boot Record** على القرص الصلب . فمثلا إذا حاول أي برنامج أن يقوم بتعديل بيانات النظام الموجودة بهذه المنطقة ، فإن الحاسب سوف يقوم بإيقاف التعامل معها مباشرة ، ثم يظهر رسالة تفيد بأن هناك برنامج يحاول تعديل بيانات النظام ، فهل توافق على هذا أم لا .

ويجب ملاحظة أن هذه الرسالة يمكن أن تظهر إذا كنت تقوم بعمل **Format** لأحد أجزاء القرص الصلب أو إذا كنت تقوم بإعادة تقسيمه ويمكن تنشيط هذا الاختيار داخل برنامج **BIOS** أو إيقافه كما يظهر بالشكل التالي :

Boot

Security Settings

Supervisor Password Installed
User Password Not Installed

Change Supervisor Password
Change User Password
Clear User Password

Boot Sector Virus Protection [Disabled]

<Enter> to change password
<Enter> again to disable password

Select Screen
↑↓ Select Item
+- Change Option
F1 General Help
F10 Save and Exit
ESC Exit

وبالطبع يختلف الشكل السابق وفقا لنــوع إصــدار برنــامج BIOS الخاص باللوحة الأم .

2. الفيروسات المقيمة :

ويطلق هذا المصطلح على نوع خاص من أنواع الفيروســات التــي تتخذ من الذاكرة المؤقتة مكانا دائما لإقامتها ، ولذلك يطلق عليها اسم الفيروسات المقيمة في الذاكرة **Resident Memory viruses** .

ويجب ملاحظة أن أي من أنواع الفيروسات التي ذكرناها سابقا يمكن أن يكون من الفيروسات المقيمة في الذاكرة .

فمن المعروف أن جميع البيانات التي يتعامل معها المعالج لابــد وأن تمر بالذاكرة المؤقتة **RAM** . وبناء على ذلك فإن مصمم الفيــروس يقوم بكتابة بعض البرامج الفرعية للفيروس التي تصيب أحد وحدات التخزين أولا – وذلك عن طريق إصابة الملفات التنفيذية أو بكتابــة نفسها مباشرة على القرص الصلب – ، ثم تقوم هذه البرامج الفرعية

بعد إصابة الحاسب ، بتحميل برنامج الفيروس الأساسي داخل الذاكرة المؤقتة في كل مرة تقوم فيها بتشغيل الحاسب ، ليبدأ الفيروس في عمله .

من المعروف أن الذاكرة المؤقتة RAM تفقد كل المعلومات الموجودة بداخلها بمجرد أن يتم إيقاف الحاسب ، فهل يعني ذلك أنه يمكن القضاء على الفيروس بمجرد إيقاف الحاسب ؟

الأمر أكثر تعقيدا من ذلك .. فبرنامج الفيروس يمكن أن يتكون من جزء واحد يقوم بعملية الإصابة ، أو يمكن أن يتكون من عدة أجزاء .
فبالنسبة للفيروسات المقيمة في الذاكرة ، نجد أن برنامج الفيروس يتكون عادة من عدة أجزاء فرعية وظيفتها التأكد من تحميل البرنامج الأساسي داخل الذاكرة المؤقتة في كل مرة تقوم فيها بتشغيل الحاسب . وهذا يعني أن الفيروس يضمن إقامة دائمة في الذاكرة المؤقتة عن طريق هذه البرامج الفرعية .

وعندما يصيب الحاسب هذا النوع من الفيروسات ، فإن الأعراض تظهر مباشرة دون حاجة إلى فترة كمون . وعادة ما تتمثل الأعراض في ظهور رسائل خطأ كثيرة كلما حاولت تشغيل أحد البرامج أو التطبيقات . مثل الرسائل الخاصة بعدم وجود ذاكرة تكفي لتشغيل التطبيقات **Not Enough Memory** .

وفكرة عمل هذا النوع من الفيروسات المقيمة في الذاكرة تقوم على أن برنامج الفيروس الأساسي يعمل على كتابة بيانات وهمية داخل الذاكرة المؤقتة ، الأمر الذي يؤدي إلى عدم وجود مساحة كافية لتشغيل التطبيقات الأخرى على الحاسب .

ويتم القضاء على هذا النوع عن طريق القضاء على البرامج الفرعية التي يستخدمها الفيروس في تحميل البرنامج الأساسي داخل الذاكرة .

فعن طريق القضاء على هذه البرامج الفرعية لن يـستمكن البرنـامج الأساسي من تحميل نفسه داخل الذاكرة .

3. الفيروسات النائمة :

عندما يتعرض الحاسب للإصابة بالفيروس ، فإن الآثـار التخريبيـة للفيروس يمكن أن تظهر مباشرة بمجرد الإصابة ، أو يظل الفيروس كامنا لفترة حتى يصيب عدد كبير من الملفـات ، ثـم تبـدأ الآثـار التخريبية له ، أو أن يكتفي الفيروس بإصابة الحاسب ثـم الانتظـار لحين تحقق شرط معين .ويطلق علـى هـذا النـوع الأخيـر اسـم الفيروسات النائمة **Sleepy viruses** .

ومن أمثلة هذا النوع الفيروس الذي أطلق عليه اسـم **CIH** ، الـذي يصيب الحاسب دون أن تظهر أعراض الإصابة إلى أن تأتي اللحظة المناسبة ليبدأ الفيروس آثاره التخريبية .

فهذا الفيروس يظل في فترة كمون حتى تاريخ 4 إبريل.، ثم يبدأ في العمل الذي يتمثل في حذف ملفات **FAT** ، أو إصابة نظام الإدخـال والإخراج الأساسي مما يؤدي إلى توقف الحاسب عن العمل في كلتا الحالتين .

ومن أمثلة هذا النوع أيضا من الفيروسات الفيروس الذي يطلق عليه اسم الفيروس الإسرائيلي **Israeli virus** ، الذي يظل في فترة كمـون

طويلة إلى اللحظة المناسبة التي تتمثل في أن يكون يوم الجمعة موافقا ليوم 13 من الشهر .

4. الفيروسات الاستعراضية :

وهو نوع خاص من الفيروسات يقوم من خلاله المبرمج باستعراض قدراته على تصميم الفيروسات ، ولكنه في واقع الأمر لا يحتوي على أية آثار تخريبية .

5. فيروسات الثغرات :

يعتمد هذا النوع من الفيروسات على الثغرات الموجودة داخل نظم التشغيل مثل نظم **Windows** بإصداراته .

ويحتاج هذا النوع من الفيروسات إلى قدرة كبيرة من المبرمج على تحليل نظام التشغيل واكتشاف الأخطاء الموجودة به ثم استغلالها ليقوم الفيروس بعمله .

ومن أمثلة هذا النوع فيروس **Stator Worm** ، حيث يقوم هذا الفيروس باستخدام **HTML Script** الموجود داخل أنظمة **Windows** فكلما قمت بفتح مجلد **Folder** من المجلدات المخزنة داخل القرص الصلب ، يقوم الفيروس بإنشاء ملفين **Folder.htt** ، **Desktop.ini** داخل هذا المجلد ، وتتكرر هذه العملية حتى يتم إنشاء أكبر عدد

ممكن من هذه الملفات التي يتم تخزينها علـــى أنهـــا **Hidden Files** داخل كل مجلد تقوم بالتعامل مع البيانات الموجودة بداخلـــه ، ممـــا يؤدي إلى بطئ شديد في التعامل مع البيانات المخزنة ، بالإضافة إلى تآكل المساحة التخزينية الخالية على القرص الصلب .

6. فيروسات الماكرو :

كلمة **Macro** تعني ملف يحتوي على مجموعة من الأوامر التي تقوم بتنفيذ وظيفة معينة . وهناك بعض أنواع الفيروسات التي يطلق عليها فيروسات الماكرو ، والتي تستخدم بشكل أساسي لإصابة الملفات التي تعمل على مجموعة برامج **Office** .

وعادة ما تصيب هذه الفيروسات الملفات الخاصة ببرنامج **Microsoft Word** ، بحيث لا يمكن التعامل مع هذه الملفات . ولكلمـــا حاولـــت القيام بتشغيلها سوف تحصل على رسالة خطأ .

7. دودة الإنترنت :

دودة الإنترنت **Internet worm** هي أحد أنواع الفيروسات التي تنتقل عبر شبكة الإنترنت . ويعتمد هذا النوع من الفيروســـت على استخدام برنامج **Outlook Express** بشكل أساسي للقيـــام بعمليـــة الانتشـــار وإصابة أكبر عدد ممكن من الأجهزة .

حيث يقوم مصمم هذا النوع من الفيروسات بزرع الفيروس داخل رسالة بريد إلكتروني ، ثم يقوم بإرسالها إلى عدد كبير من مستخدمي الشبكة يقوم باختيارهم بشكل عشوائي . وبمجرد أن يقوم الضحية بفتح الرسالة ، يبدأ الفيروس في الحصول على دفتر العناوين Address Book الخاص بالضحية – الذي يحتفظ بداخله بعناوين البريد الإلكتروني الخاص بأصدقائه – ثم يقوم باستخدام البريد الإلكتروني الخاص بالضحية في إرسال رسائل إلى أصدقائه تحتوي على الفيروس .. وبهذا لن يشك مستلم الرسالة في أنها تحتوي على فيروس ، حيث أنه يعرف الراسل . وبالتالي يضمن الفيروس انتشارا كبيرا حول العالم .

8. برامج التجسس :

من الأخطاء الشائعة أن نعامل برامج التجسس Spy wares على أنها نوع من الفيروسات التي تصيب الحاسب .

فهذا النوع من البرامج لا يتشابه مع الفيروس إلا من حيث أن كلاهما يقوم بالتسلل وإصابة الحاسب دون رغبة المستخدم ، ولكن برامج التجسس لا تقوم بإصابة الحاسب بأية آثار تخريبية كما يحدث بالنسبة للفيروس .

فهذه البرامج تصيب الحاسب بغرض التجسس علـــى المعلومـــات ، وعادة ما تستهدف هذه البرامج الشركات الصناعية الكبيرة بغــرض التجسس على الأبحاث العملية الخاصة بها ، أما بالنســبة للمســتخدم العادي فلا تمثل له هذه الأهمية الكبيرة ..

الفصل الخامس

البرامج المضادة للفيروس

الفصل الخامس

البرامج المضادة للفيروسات

في الوقت الذي أقوم فيه بكتابة هذا الكتاب ، قمت بنقل بعض البيانات المصابة فيروس **WIN32/CIH** ، وذلك لاختبار قدرة البرامج المضادة للفيروسات على اكتشاف هذا الفيروس والتخلص منه .

وقد استخدمت لإجراء هذه التجربة ثلاث برامج مضادة للفيروسات ، هي :

1. برنامج **Norton Anti virus 2004** بأحدث مكتبة مضادة للفيروسات قمت بالحصول عليها من خلال شبكة الإنترنت .
2. برنامج **AVG 6** وهو أحد البرامج المجانية التي يمكن الحصول عليها من خلال شبكة الإنترنت ، بالإضافة إلى أنني قمت بتحديث هذا البرنامج أيضا من خلال موقع الشركة المنتجة للبرنامج .
3. برنامج **Pest Patrol** ، وهو برنامج تجريبي **Trail Version** متخصص في اكتشاف الفيروسات وبرامج التجسس .. مع العلم أن النسخة التجريبية تستطيع الكشف عن أماكن وجود الملفات المصابة دون علاجها أو حذفها .

هل تعلم ماذا كانت النتيجة ؟

نتيجة تثبيت البرامج السابقة على الحاسب المصاب كانت كالتالي :

1. برنامج Norton Anti virus بمجرد تثبيته علـى الحاسب المصاب ، يطلب منك أن تقوم بإعادة تشغيل الحاسب حتـى تكتمل عملية التثبيت . وبمجرد إعادة تشغيل الحاسب ، بـدأ ظهور عدد من الرسائل الخاصة بالبرنامج تفيد بأن الفيروس قد أصاب البرنامج نفسه وأنه غير قادر على العمـل !! ثـم عرض البرنامج رسالة أخرى تفيد بأنه يجب أولا اسـتخدام Rescue Disk الخاص به حتى تتمكن مـن حـذف ملفـات الفيروس عن طريق نظام DOS !! والأمر الأكثر عجبـا أن البرنامج قام بإيقاف عمل نظام التشغيل الموجود على الحاسب لتلافي حدوث المزيد من الأضرار .
2. بالنسبة لبرنامج AVG استطاع هذا البرنامج أن يقوم بتصليح Repair معظم الملفات المصابة ، وبعـد عمـل Full Scan للحاسب بواسطة هذا البرنامج ، كانت نتيجة هذه العمليـة أن قام البرنامج بعرض تقرير يفيد أن البرنامج استطاع التخلص من الفيروس نهائيا . ولكن الأمر العجيب أنه حينما حاولـت القيام بتشغيل بعض الألعاب ، قام البرنامج بعرض رسالة تفيد بأن هذه اللعبة مازالت مصابة بالفيروس ، واقترح أن يقـوم إما بالسماح بتشغيل الملف المصاب ، أو عدم السماح بتشغيله أو القيام بعلاج الملف المصاب .. وكلما قمت بالضغط علـى

مفتاح علاج الملف المصاب Heal ، تظهر رسالة أخرى تفيد بأنه غير قادر على علاج هذا الملف .. والاختيار لك !!!

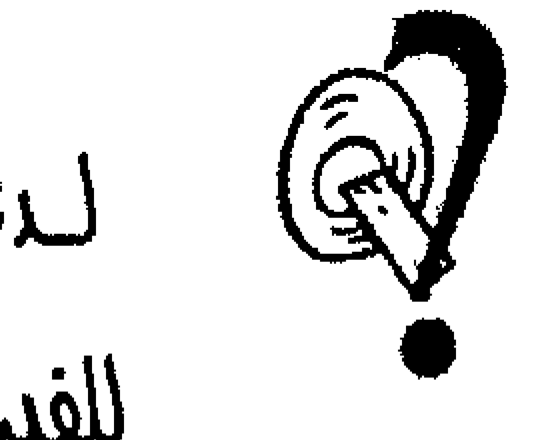
3. أما بالنسبة لبرنامج Pest Patrol ، فهو برنامج رائع حقا لــو أن لديك النسخة الكاملة منه . فقد كشف هذا البرنــامج عــن أماكن الملفات المصابة بدقة متناهية ، بالإضافة إلى أنه كشف عن وجود نوعين من برامج التجسس التي أصابت الحاســب نتيجة نقل البيانات المصابة بالفيروس .. ولكنه بالطبع اكتفي بهذا التقرير الدقيق ولم يقوم بإزالة هذه الملفات أو علاجها .

والآن .. ما الذي نستخلصه من هذه التجربة ؟

لا شيء في الواقع ، فتوقف برنامج Norton عن العمل بمجرد تثبيته على الحاسب المصاب لا يعني أنه برنامج سيئ ، بل يعني أن هــذا البرنامج مثل أي برنامج آخر له بعض المميزات والعيوب .

إذا .. ما هو أفضل برنامج مضاد للفيروسات يمكن استخدامه ؟

لن أجيبك على هذا السؤال ، بل سوف أترك لك الاختيار



لدى سؤال آخر .. ما هي فكرة عمل البرامج المضادة للفيروسات ؟

هذا السؤال أستطيع أن أجيب عليه الآن ..

أي برنامج مضاد للفيروسات عادة ما يتكون من جزأين

الجزء الأول : وهو البرنامج الأساسي ، ووظيفة هذا البرنامج هو البحث داخل ملفات النظام عن الملفات المصابة بالفيروس ، ثم علاج هذه الملفات أو حذفها أو حجبها حتى لا تستطيع التعامل معها .

الجزء الثاني : عبارة عن مكتبة يطلق عليها **Virus definition** . فعندما يظهر فيروس جديد ، تقوم الشركات المنتجة لهذه البرامج بالحصول على نسخه من الملفات المصابة ، ثم تقوم بمقارنتها بملفات غير مصابة ، حتى تستطيع التعرف على مجموعة الأوامر التي يقوم الفيروس بكتابتها داخل الملفات المصابة .

ثم يتم حصر هذه الأوامر وإضافتها إلى مكتبة **Virus Definition** حتى يستطيع البرنامج التعرف على الفيروس في حالة وجودة على الحاسب .



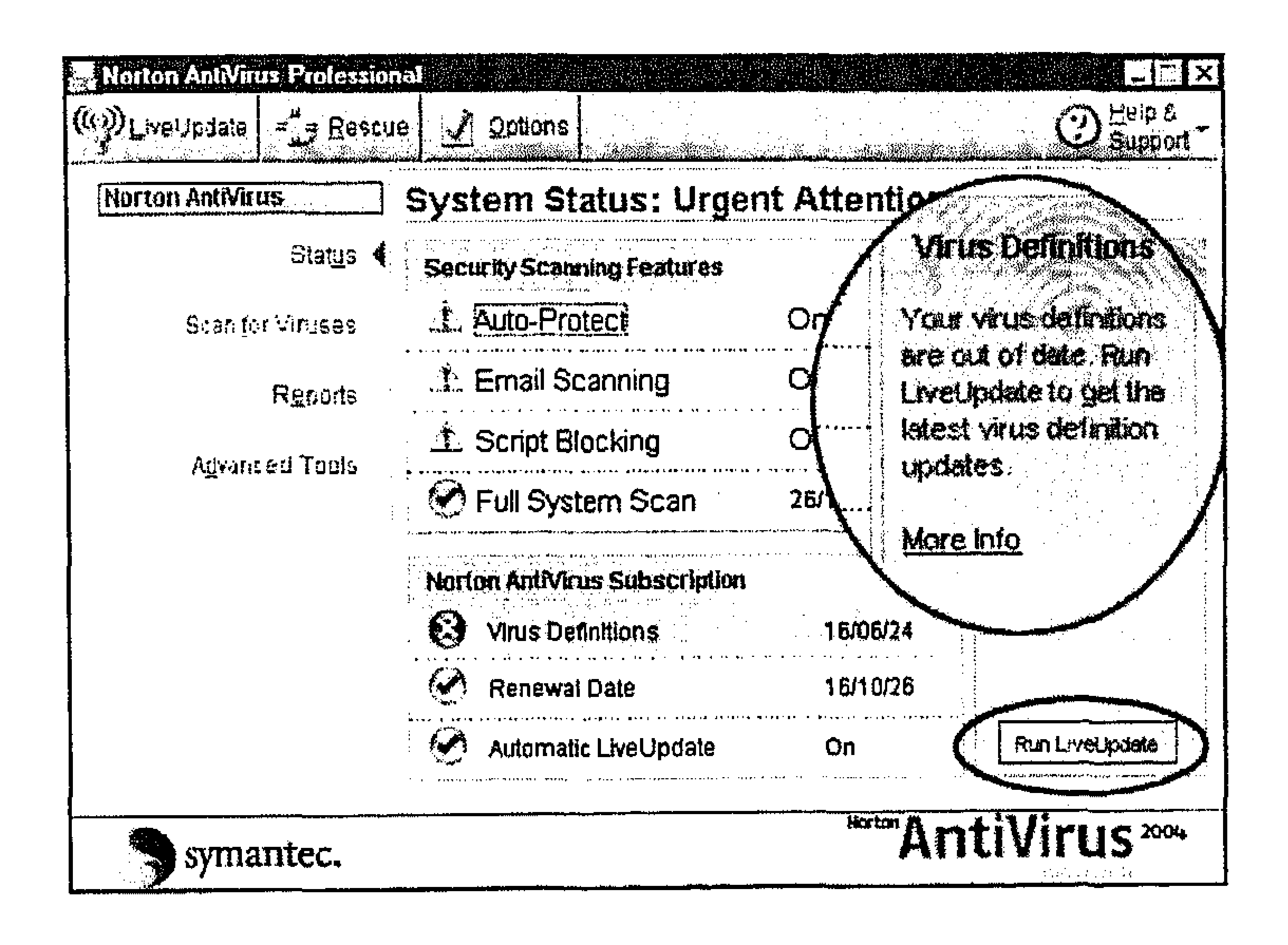
هل أفهم من ذلك أنه إذا لم تكن هذه المكتبة تم تحديثها في وقت قريب فإن هذا يعني أنه يوجد احتمال وجود فيروس على الحاسب على الرغم من وجود برنامج مضاد للفيروسات مثبت على النظام ؟

لا .. لا يوجد فقط احتمال وجود فيروس . بل أن هذا ما يحدث في معظم الأوقات ، فكثيرا ما يطمئن المستخدم نظرا لوجود برنامج مضاد للفيروسات على الحاسب ، ويكتشف بعد ذلك أن الحاسب الخاص به مصاب بنوع من الفيروسات أو برامج التجسس !!

تخيل معي أنك قمت بتثبيت برنامج 2004 **Norton** الذي بدأ ينتشر وجوده في العالم العربي من وقت قصير . هل تعلم أن هذا الإصدار من البرنامج قد قامت الشركة بإطلاقه في نهاية عام 2003 ؟

هل تعلم أن شركة **Symantec** التي تنتج هذا البرنامج قد قامت بإطلاق الإصدار 2005 ؟

هل لاحظت يوما هذه الرسالة التحذيرية الصغيرة التي تظهر كلما قمت بتشغيل برنامج **Norton 2004** ؟



هذه الرسالة تطلب منك الدخول على شبكة الإنترنت ، ثـم الضـغط على مفتاح **Run Live update** للحصول علـى آخـر إصـدارات **Virus Definition** ، حتى لا تتعرض لخطر وجود فيـروس علـى الحاسب دون أن يشعر البرنامج بوجوده .

إذا ، بغض النظر عن البرنامج الذي تستخدمه ، إذا لم تقوم بتحـديث **Virus Definition** بشكل دوري ، فإن هذا يعنـي احتمـال إصـابة الحاسب بالفيروس دون أن يشعر البرنامج بوجوده .. وبالمثل فإن هذا يعني أنه يمكنك استخدام برنامج **Norton 2001** مثلا باطمئنـان تـام طالما أنك تقوم بتحديث مكتبة الفيروسات الخاصة به بشكل مستمر.

والآن نعود لموضوعنا الأساسي حول أفضل برنامج يمكن استخدامه ، وللإجابة على هذا التساؤل ، سوف نفرق بين حالتين ..

الحالة الأولي – إذا كان الحاسب غير مصاب بالفيروس :

إذا كان الحاسب غير مصاب بالفيروس وترغب في استخدام برنامج مضاد للفيروسات يضمن لك عدم الإصابة ، فيجب عليك فـي هـذه الحالة استخدام أي من إصدارات برنامج **Norton** – مع العلـم أنـه يفضل استخدام الإصدارات الحديثة إذا كانت متاحة – وذلك للأسباب الآتية :

1. إن هذا البرنامج صمم خصيصا لضمان عدم إصابة الحاسب بالفيروس سواء أثناء تبادل البيانات بواسطة وحدات التخزين أو عن طريق شبكة الإنترنت .
2. على الرغم من أن تثبيت هذا البرنامج على الحساب يؤدي إلى بطء في التعامل مع النظام أو أثناء فترة التحميل ، إلا أنه يحتوي على العديد من الإمكانيات التي تجعل من هذا البطء أمر قابل للاحتمال .
3. من أهم مميزات هذا البرنامج أن شركة **Symantec** تقوم بتحديث مكتبة الفيروسات الخاصة بها على شبكة الإنترنت بشكل دوري وبمجرد ظهور فيروسات جديدة .
4. عملية تحديث مكتبة الفيروسات يمكن أن تتم عن طريق الضغط على مفتاح **Run Live update** مباشرة ، وفي هذه الحالة سوف يقوم البرنامج – بشكل تلقائي – بالاتصال بموقع الشركة المنتجة على الشبكة ، والبحث عن أي تحديث يمكن تثبيته . وفي هذه الحالة سوف يقوم البرنامج بتحديث مكتبة الفيروسات مباشرة داخل نظام التشغيل ، وهذا يعني أنه في حالة تثبيت نظام تشغيل جديد ، سوف تضطر إلى إعادة هذه العملية مرة أخري .. كما توجد طريقة أخرى لتحديث هذه المكتبة عن طريق الدخول على موقع شركة **Symantec** ، والحصول على ملف يحتوي على أحدث مكتبة للفيروسات .

وفي هذه الحالة يمكنك الاحتفاظ بهذا الملف وإعادة تثبيته إذا قمت بتغيير نظام التشغيل في أي وقت .

5. من أهم مميزات هذا البرنامج أن عملية تحديث **Virus definition** عملية مجانية لا تتقاضى عنها الشركة المنتجة أية مصاريف ، وذلك بعكس بعض البرامج الأخرى مثل برنامج **Macafee Virus scan** وهو برنامج فعال للغاية ولكن الشركة المنتجة لهذا البرنامج تصر على تقاضى أجر مقابل تحديث هذا البرنامج .

إذا ، خلاصة ما سبق أن برنامج **Norton** من البرامج الفعالة للغاية إذا كان الحاسب غير مصاب ، ولكنه أظهر فشلا في حالة تثبيته على حاسب مصاب بالفيروس لأنه كما ذكرنا من قبل بمجرد تثبيته سوف يؤدي إلى تعطيل نظام التشغيل .

الحالة الثانية – إذا كان الحاسب مصاب بفيروس :

إذا كان الحاسب مصاب بفيروس ، فينصح في هذه الحالة باستخدام واحد من الأساليب الآتية للتخلص من آثار الفيروس :

1. إذا كنت تعلم اسم الفيروس الموجود على الحاسب ، فيمكنك في هذه الحالة الحصول على مضاد لهذا الفيروس فقط من خلال موقع شركة **Symantec** . حيث تقوم هذه الشركة

بإنتاج ملفات مخصصة لإزالة نوع معين من الفيروسات ، وهي أيضا خدمة مجانية تقدمها الشركة .

2. إذا كنت لا تعرف اسم الفيروس ، ففي هذه الحالة يمكنك تثبيت برنامج **AVG** أو برنامج **Anti VIR** . فهذه البرامج تتميز بأنها صغيرة الحجم ومجانية ، ويمكنك الحصول عليها عن طريق المواقع المختلفة داخل شبكة الإنترنت .

3. إذا لم تتمكن البرامج السابقة من إزالة الفيروس ، فيمكنك في هذه الحالة أن تقوم بإزالة نظام التشغيل الموجود ، ثم تثبته مرة أخرى . وهذه الطريقة سوف تمنحك بعض الوقت حتى يصيب الفيروس ملفات النظام الجديد ، وبهذا يمكنك تثبيت برنامج **Norton** وتحديثه من خلال موقع الشركة ، ثم عمل مسح شامل **Full Scan** للحاسب .. وسوف تنجح هذه الطريقة إلا إذا كان الفيروس الذي أصاحب الحاسب من نوعية الفيروسات المقيمة في الذاكرة .

4. إذا قمت بكل الخطوات السابقة ولم تنجح في إزالة الفيروس ، فيمكنك أن تقوم بتثبيت برنامج **Norton** مثلا على أي حاسب غير مصاب بالفيروس ، ثم تقوم بإنشاء **Rescue disk** واستخدامها على الحاسب المصاب . ولكن هذا الأسلوب سوف يتطلب منك معرفة بكيفية استخدام نظام **DOS** ، كما أن هذه الطريقة سوف تأخذ وقتا طويلا .

5. أما آخر طريقة يمكنك أن تلجأ إليها للتخلص من الفيـــروس فهي أن تقوم بتوصيل القرص الصلب **Hard Disk** الخـــاص بالحساب المصاب ، بجهاز آخر مثبت عليه برنامج **Norton** ثم تقوم بعمل مسح شامل لجميع وحدات التخـــزين المتصـــلة بالحاسب .
6. إذا لم تستطع إزالة الفيروس بعد كل المحـــاولات الســـابقة ، فأنت بالتأكيد تحتاج إلى متخصص في الصيانة .

الفصل السادس

التخلص من الفيروس

الفصل السادس

التخلص من الفيروس

التخلص من الفيروس يعتمد بشكل أساسي على استخدام برنامج مضاد للفيروسات ، وعلى الرغم من المزايا والعيوب الخاصة ببرنامج Norton التي ذكرناها خلال الفصل السابق ؛ إلا أن هذا البرنامج من أكثر البرامج المضادة للفيروسات التي يمكنك الاعتماد عليها ، كما أنه البرنامج الأكثر انتشارا بين المستخدمين نظرا لأنه برنامج مجاني . لذلك ، فإننا سوف نتعرض في هذا الفصل إلى بعض النقاط الخاصة بهذا البرنامج ، مع العلم أننا سوف نستخدم الإصدار 2004 .

Rescue Disk :

ما المقصود بعبارة Rescue Disk ؟
يقصد بـ **Rescue Disk** ملفات الإنقاذ التي يقوم برنامج **Norton** بتخزينها على بعض الأقراص المرنة **Floppy Disks** ، حيث يمكن لهذه الملفات العمل من خلال نظام تشغيل **Dos** . وتصل عدد الأقراص المرنة التي يحتاجها الإصدار **2004** لإنشاء **Rescue Disk** إلى 8 ، بينما في الإصدارات السابقة مثل 2003 كانت عدد الأقراص المرنة التي يحتاجها البرنامج هي 3 .

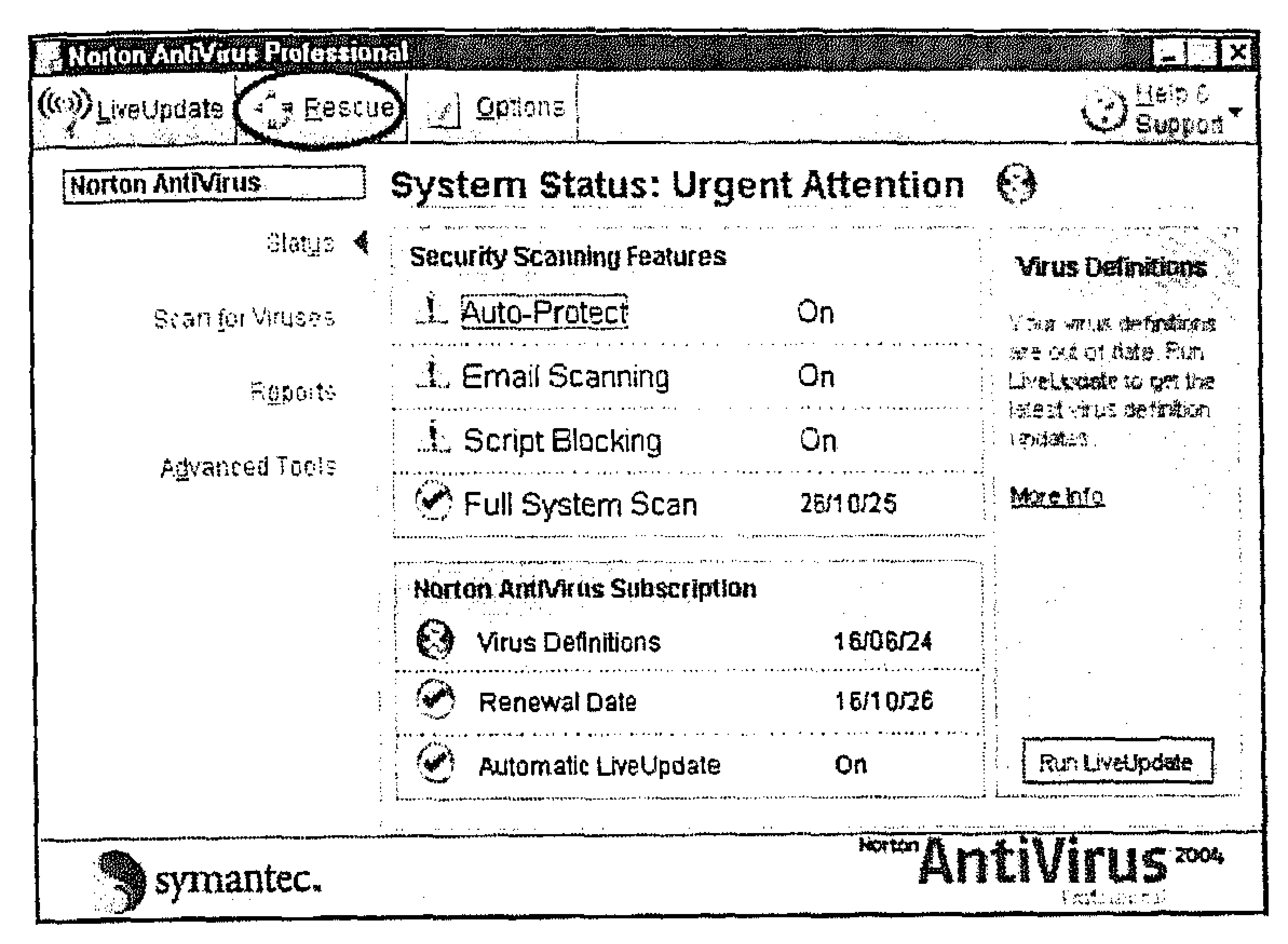
وقد كانت شركة Symantec من أولي الشركات التي قامت بإضافة هذه الخاصية إلى برامجها .

تخيل معي أن الفيروس قام بتخريب نظام التشغيل . فكيف يمكنك في هذه الحالة أن تقوم بإزالة الفيروس ؟

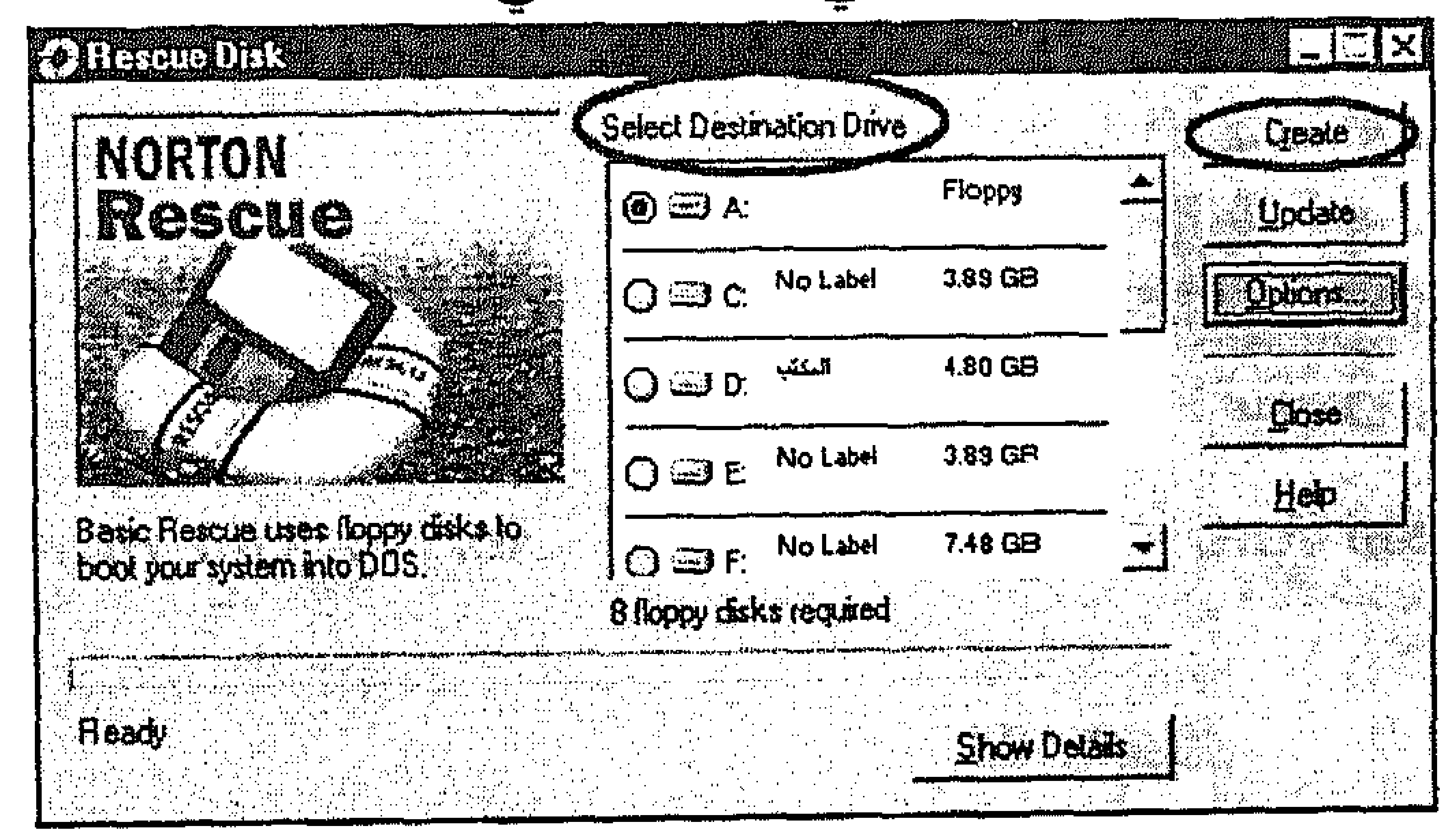
فلنفترض أن الفيروس لم يقوم بتخريب نظام التشغيل ، ولكنه قام بنسخ نفسه داخل بعض ملفات نظام التشغيل التي يتم تحميلها داخل الذاكرة المؤقتة بمجرد تشغيل النظام ، فكيف يستطيع برنامج **Norton** أو أي برنامج آخر في هذه الحالة أن يقوم بإزالة الفيروس مع هذه الملفات ؟ مع العلم أن نظام التشغيل لن يسمح لأي برنامج أن يقوم بالتعديل في هذه الملفات طالما أنها موجودة داخل الذاكرة المؤقتة .
إذا استخدام **Rescue Disk** من خلال نظام **Dos** أمر لا غنى عنه ..

خطوات إنشاء **Rescue Disk** :

1. اضغط مرتين بالمفتاح الأيسر للماوس على الأيقونة الخاصة ببرنامج **Norton** الموجودة في شريط المهام ، أو من خلال القائمة **Start** ، اختر **Programs** ، ثم انتقل إلى **Norton Anti virus** ، واختر منها **Norton Anti virus professional** .
2. سوف تظهر النافذة الرئيسية للبرنامج ، كما في الشكل التالي:



3. اضغط مفتاح **Rescue** ، فتظهر النافذة الخاصة بإعداد **Rescue Disk** كما في الشكل التالي :



من خلال القائمة **Select Destination Drive** يمكنك اختيار تخزين هذه الملفات على أقراص مرنة – وهو الوضع الافتراضي– أو تخزينها داخل أي مجلد على أحد أجزاء القرص الصلب .

ويجب ملاحظة أن :

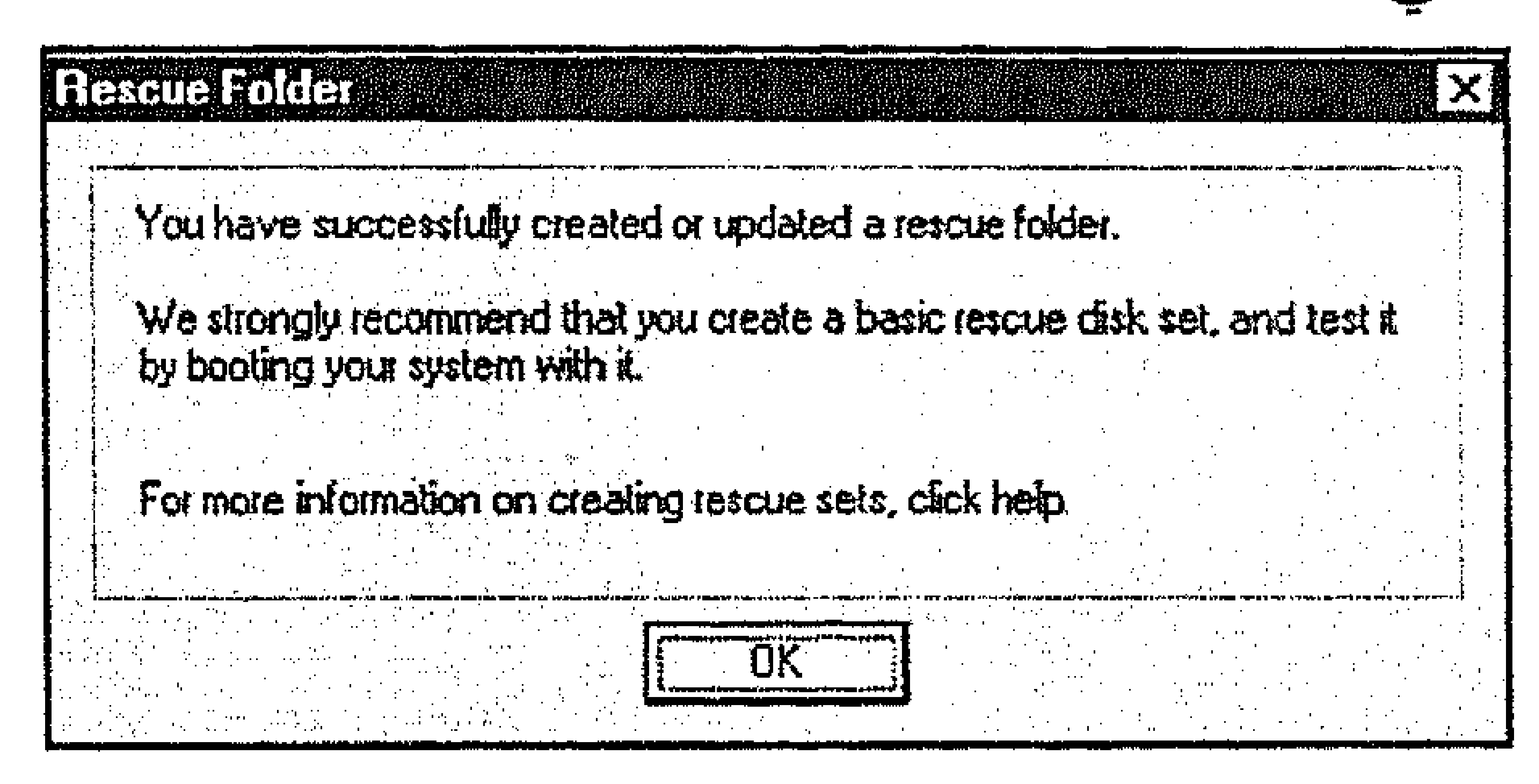
- لابد من إنشاء هذه الملفات عندما يكون الحاسب غير مصاب بالفيروس .
- لا يفضل الاحتفاظ بهذه الملفات على أحد أجزاء القرص الصلب إلا إذا كنت تملك **Writer** ، وسوف تقوم بنقل هذه الملفات إلى أسطوانة مدمجة **CD** .
- في حالة تخزين ملفات الإنقاذ على أقراص مرنة ، فتأكد من عمل **Format** لهذه الأقراص قبل نسخ الملفات إليها .

4. إذا كنت تستخدم أقراص مرنة ، فأدخل القرص الأول ثم اضغط مفتاح **Create** . أما في حالة تخزين هذه الملفات على أحد أجزاء القرص الصلب ، فقم بتحديده ، ثم اضغط مفتاح **Create** . وفي هذه الحالة سوف تظهر نافذة أخرى على الشكل التالي :

Select Rescue Folder	
Rescue Path: K:\Rescue	OK
Enter Rescue folder name: Rescue ...	Cancel

ويمكنك من خلال هذه النافذة تحديد اسم المجلد الذي سوف يتم حفظ الملفات بداخله .

5. اضغط مفتاح **Ok** ، وسوف يبدأ البرنامج في إعداد ملفات الإنقاذ.
6. في نهاية عملية الإعداد سوف تظهر رسالة على الشكل التالي:



حيث تفيد هذه الرسالة بأن عملية إعداد **Rescue Disk** قد تمت بنجاح وتنصحك بتجربة هذه الملفات .

استخدام Rescue Disk :

إذا قمت بإعداد **Rescue Disks** على أقراص مرنة ، ففي هذه الحالة ، يمكنك استخدامها بالشكل التالي :

1. قم بإعادة تشغيل الحاسب ، مع وضع القرص الأول داخل وحدة الأقراص المرنة **Floppy Drive** .
2. إذا لم يقوم الحاسب بتحميل ملفات النظام الموجودة على هذا القرص ، فعليك في هذه الحالة تغيير تتابع التحميل **Boot Sequence** الخاص بالحاسب عن طريق الدخول إلى برنامج

BIOS – وذلك بإعادة تشغيل الحاسب مرة أخرى مع استمرار الضغط على مفتاح **Delete**– ثم اختيار العنصر **Load Setup Defaults** ، ثم الخروج من برنامج **BIOS** عن طريق الضغط على مفتاح **F10** أو اختيار العنصر **Save & Exit Setup** .

3. سوف يقوم الحاسب بقراءة الملفات الموجودة على القرص الأول ، ثم يطلب منك إدخال القرص الثاني .. وتستمر هذه العملية حتى ينتهي النظام من قراءة جميع الأقراص .
4. بعد الانتهاء من قراءة جميع الأقراص المرنة ، سوف يبدأ برنامج الإنقاذ في العمل .



عندما حاولت القيام بهذه الطريقة ، لم ينجح الحاسب في قراءة أحد الأقراص المرنة التي قمت بإعدادها ، فما هو الحل ؟

مشكلة الأقراص المرنة منذ أن ظهرت أنها سريعة التلف ولا يمكن الاعتماد عليها في نقل البيانات .

فإذا تعرضت إلى مثل هذه المشكلة ، فعليك في الحالة أن تقوم بإنشاء **Rescue Disk** على أحد أجزاء القرص الصلب ، ثم تقوم بنقلها إلى أحد الأقراص المدمجة **CD** .. ولكن ، إذا قمت بذلك فسوف تظهر أمامك مشكلة أخرى !! وهي أن عملية الإنقاذ لن تبدأ بشكل تلقائي في

هذه الحالة ، بل يجب عليك أن تقوم بتشغيل عملية الإنقاذ عن طريق استخدم بعض أوامر **DOS** .

لا تقلق .. الأمر ليس بهذا التعقيد ، فيمكنك القيام بهذه العملية عن طريق الخطوات التالية :

1. قم بإعداد **Startup Disk** على أحد الأقراص المرنة ، وذلك عن طريق اختيار العنصر **Add/Remove Programs** من داخل **Control Panel** . فتظهر نافذة تحتوي في الجزء العلوي منها على ثلاث علامات تبويب ، فانتقل إلى علامة التبويب الأخيرة **Startup Disk** ، ثم اضغط مفتاح **Create Disk** .
2. أعد تشغيل الحاسب ، وبعد قراءة ملفات النظام الأساسية من خلال **Startup Disk** . سوف تظهر أمامك ثلاث اختيارات خاصة بعملية التحميل .
3. انتقل إلى الاختيار الأول **Start With CD-ROM support** ثم اضغط مفتاح **Enter** .
4. قم بإدخال القرص المدمج الذي يحتوي على ملفات الإنقاذ – وليكن اسمه **K**– ثم اكتب الأمر التالي :

```
A:\> K:
```

ثم اضغط مفتاح **Enter** .

5. انتقل إلى المجلد الذي يحتوي على ملفات الإنقـــاذ ، والـــذي يحمل اسم **Rescue** ، عن طريق كتابة الأمر التالي :

```
K:\> cd rescue
```

ثم اضغط مفتاح **Enter** .

6. لبدأ عملية الإنقاذ ، قم بكتابة الأمر التالي :

```
K:\Rescue> navdx /all /doallfiles /repair /heur:3
```

ثم اضغط مفتاح **Enter** كما في الشكل التالي :

```
K:\>cd rescue

K:\Rescue>navdx /all /doallfiles /repair /heur:3
Loading NAVDX, please wait...
Using virus definitions from C:\...~1\COMMON~1\SYMANT~1\VIRUSD~1\20030814.007
Using options from K:\RESCUE

Scanning Memory... OK
Scanning Master Boot Records... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
Scanning Boot Record... OK
```

ويتكون الأمر السابق من عدة أجزاء كالتالي :

navdx	وهو اسم الملف التنفيذي الذي يبدأ عملية الإنقاذ
/all	معامل خاص بوحدات التخزين التي سوف يـــتم فحصـــها ، حيث يشير المعامل All إلى فحص جميع وحدات التخـــزين الموجودة بالحاسب ، ويمكن استبدال هذا المعامل باسم أحـــد أجزاء القرص الصلب مثلا ، ويصبح الأمر في هذه الحالـــة على الشكل التالي:

```
Navdx C: /doallfiles /repair / heur:3
```

/doallfiles	يستخدم هذا المعامل لفحص جميع أنواع الملفات ، حيث أن الوضع الافتراضي أن يتم فحص الملفات التي يحتمل إصابتها بكثرة مثل الملفات التنفيذية
/repair	والواضح من الاسم أن هذا المعامل خاص بعلاج الملفات المصابة بشكل تلقائي في حالة اكتشافها . ويمكنك تغيير هذا المعامل إلى delete ليقوم البرنامج بحذف الملفات المصابة ، أو Prompt ليقوم البرنامج بعرض رسالة تسألك ما إذا كنت ترغب في حذف الملفات المصابة أو علاجها أو حجبها عن التعامل . وعلى ذلك يمكن استخدام الأمر السابق بأحد الأشكال التالية:

```
Navdx /all /doallfiles /delete /heur:3
Navdx /all /doallfiles / prompt / heur:3
```

Heur:3	يقوم هذا المعامل بتشغيل خاصية يطلق عليها اسم Blood hound ، حيث تعمل هذه الخاصية على القيام بفحص دقيق للملفات والبحث عن احتمالات الإصابة في حالة شك البرنامج في أن أحد الملفات مصاب بفيروس ولكنه لا يستطيع التعرف عليه . ويمكنك بالطبع تجاهل هذا المعامل لأنه يؤدي إلى طول فترة عملية الفحص .

وعند الانتهاء من البحث داخل كل وحدة من وحدات التخزين ، سوف يقوم البرنامج بعرض تقرير عن نتيجة عملية البحث ، كما في الشكل التالي:

```
Summary:               No Viruses Found
Items Scanned:         C:-K:
File Type:             All Files
Scan Time:             2 minutes, 4 seconds

Item                       Scanned    Infected    Cleaned
-----------------------    ---------  ----------  ---------
Memory:                    Yes        No          --
Master Boot Records:       2          0           --
Boot Records:              9          0           --
Files:                     4911       0           --
```

الحجر الصحي :

عند التعامل مع برنامج **Norton** عادة ما تلاحظ أن هناك كلمة تترد كثيرا يطلق عليها **Quarantine** وهي تعني الحجر الصحي ، وتنطق [كوارنتين] . وعلى الرغم من أهمية هذه الخاصية داخل البرنــامج ، إلا أن الكثير لا يعرف كيفية الاستفادة منها .

فعندما ينتهي البرنامج من فحص وحدات التخزين الموجودة بالحاسب ، تأتي مرحلة معالجة الملفات المصابة والتي تمــر بــدورها بعــدة مراحل فرعية كالتالي :

المرحلة الأولي : وهي مرحلة معالجة الملفات المصابة عن طريــق إزالة أوامر الفيروس من داخل كل ملف مصـــاب . وفي حالة عدم قدرة البرنامج عــن إزالـــة أوامــر الفيروس ، فإنه ينتقل إلى المرحلة الثانية .

المرحلة الثانية : يقوم البرنامج خلال هذه المرحلة بعرض اختيارين للمستخدم للتصرف في الملفات المصـــابة .. **الاختيار الأول** هو **Quarantine** : ويعني هـــذا الاختيـــار أن

البرنامج سوف يقوم بعزل الملفات المصابة داخل مجلد خاص بالبرنامج بحيث لا يسمح للمستخدم بالتعامل معها . وقد تكون هذه الملفات مصابة بفيروس ولكن البرنامج لا يستطيع التخلص منه ، أو قد يحتمل إصابتها بفيروس لا يستطيع البرنامج التعرف عليه . أما **الاختيارالثاني** فهو **Delete** : ويعني أن يقوم البرنامج بحذف الملفات المصابة نهائيا من الحاسب ، ويلاحظ أن هذا الاختيار فعال للغاية في إزالة الفيروس ، ولكنه يؤدي إلى فقد العديد من البرامج التي قد يحتمل وجودها على الحاسب ، كما أنه يؤدي إلى إحداث خلل بنظام التشغيل .



إذا ، ما هي خطورة استخدام خاصية **Quarantine** ؟

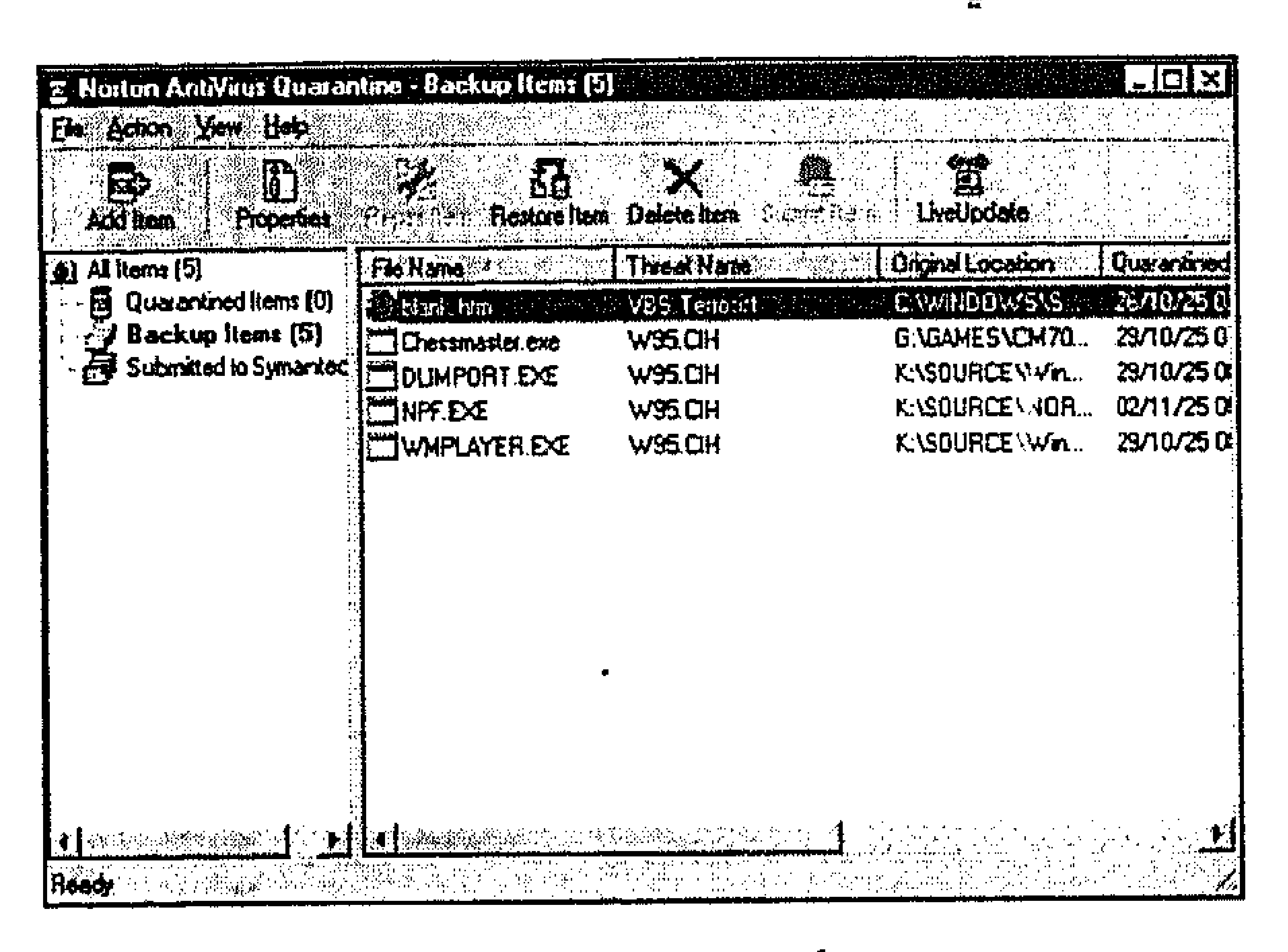
خطورة استخدام هذه الخاصية تتمثل في أنه بعد فترة سوف تلاحظ عدم وجود مساحة كافية لتشغيل البرامج على الجزء :C من القرص الصلب . وذلك لأن برنامج **Norton** يقوم بعمل نسخ من الملفات التي تم حجرها صحيا وعزلها داخل مكان خاص على الجزء **:C** .



وهنا يأتي السؤال التالي .. كيف يمكنه التخلص من الملفات الموجودة داخل الحجر الصحي ؟

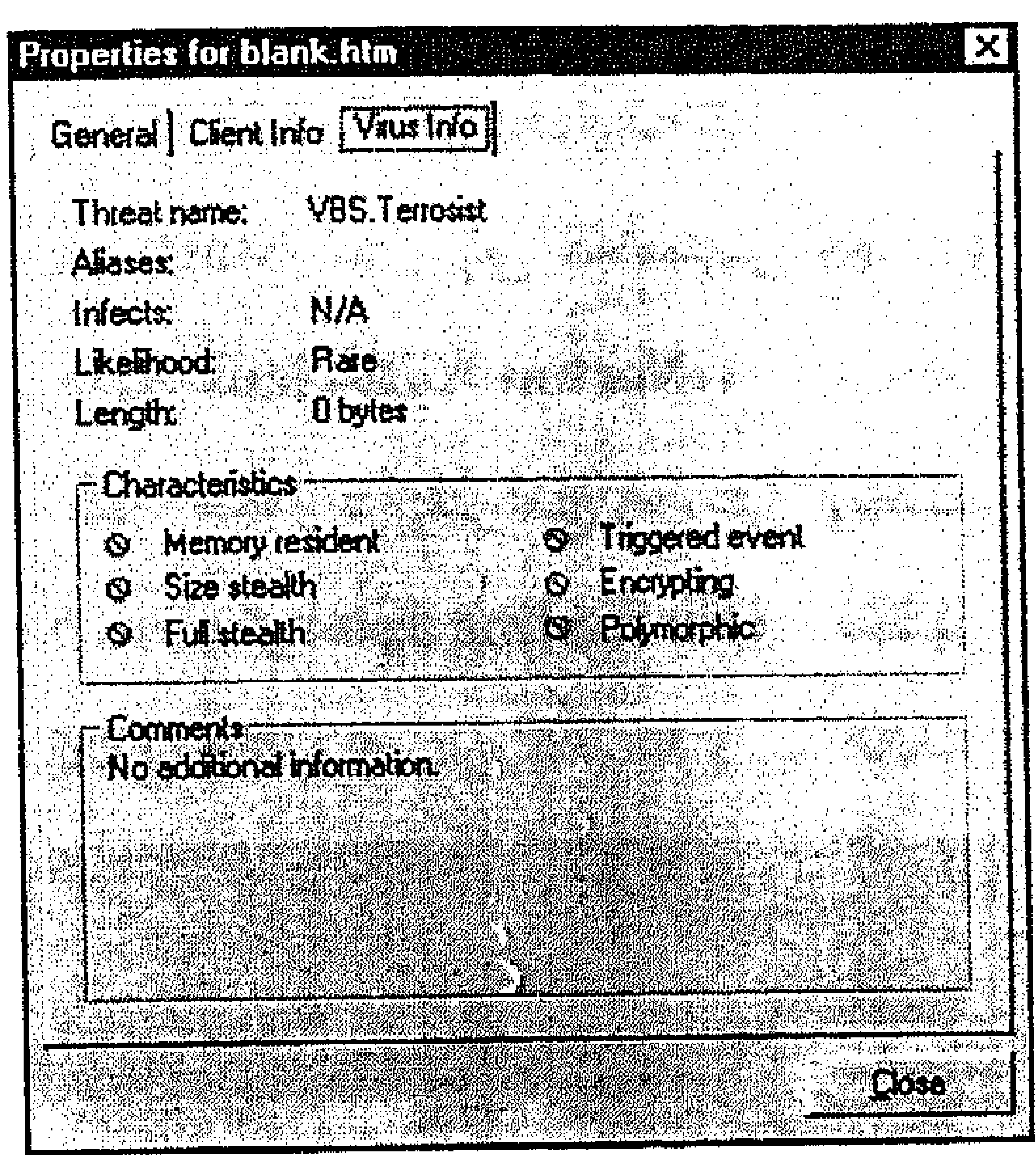
يمكن التخلص من هذه الملفات عن طريق الخطوات التالية :

1. من القائمة Start انتقل إلى العنصر Programs ، ومنها اختر برنامج **Norton Anti virus** .
2. سوف تظهر مجموعة البرامج الفرعية المصاحبة لبرنامج Norton ، فاختر منها **Quarantine** . فتظهر نافذة على الشكل التالي :



ويظهر داخل هذه النافذة أسماء الملفات التي تم عزلها ، وبجانب كل ملف بعض البيانات عنه مثل نوع الفيروس الذي أصاب الملف .

كما يمكنك التعرف على المزيد من المعلومات الخاصة بالملف عن طريق الضغط على مفتاح **Properties** ، فتظهر نافذة كما في الشكل التالي :



ومن خلال هذه النافذة يمكنك الضغط على علامة التبويب **Virus Info** ليظهر لك بعض المعلومات الإضافية حول الفيروس .

3. لحذف الملفات التي تم عزلها ، اضغط مفتاحي **Ctrl +A** لتحديد جميع الملفات ، ثم اضغط مفتاح **Delete Items** .

حماية سلة المحذوفات :

عند تثبيت برنامج **Norton** على الحاسب ، يقوم البرنامج بعمل حماية للملفات التي يتم إرسالها إلى سلة المحذوفات **Recycle bin** .

وعندما تقوم بحذف الملفات الموجودة داخل سلة المحذوفات عن طريق استخدام الأمر **Empty Recycle Bin**، فإن البرنامج يقوم بالاحتفاظ بهذه الملفات داخل مكان خاص على القرص الصلب ، بغرض إمكانية استعادتها مرة أخرى .

وهذا يعني أنك يجب عليك بين فترة وأخرى أن تقوم بالتخلص من هذه الملفات عن طريق الخطوات التالية :

1. من سطح المكتب **Desktop** انتقل إلى الأيقونة الخاصة بسلة المحذوفات **Recycle bin** .
2. اضغط بالمفتاح الأيمن للماوس ، فتظهر قائمة على الشكل المقابل :
3. اضغط الاختيار **Empty Norton Protected files** .

Open
Explore
Scan Directory with PestPatrol
UnErase Wizard
Empty Recycle Bin
Empty Norton Protected Files
FastFolders
Create Shortcut
Properties

ملحوظة هامة ...

عند إزالة تثبيت برنامج **Norton** يجب مراعاة إزالة الملفات التي تم عزلها بواسطة خاصية **Quarantine** بالإضافة إلى إزالة الملفات المحمية داخل سلة المحذوفات .

الفصل السابع

الفيروس فى نقاط

الفصل السابع

الفيروس في نقاط

سوف نقوم خلال هذا الفصل بعرض سريع لأهم النقاط التي جاءت في الفصول السابقة بشكل مختصر...

- الفيروس هو عبارة عن برنامج يحتوي على مجموعة من الأوامر .
- ينتقل الفيروس إلى الحاسب عن طريق نقل البيانات المصابة سواء عن طريق تداولها من خلال وسائط التخزين المختلفة أو عن طريق شبكة الإنترنت .
- عندما يصيب الفيروس الحاسب ، فإن هناك بعض الأعراض التي يمكن من خلالها التعرف على وجود الفيروس مثل :
  - بطء شديد في التعامل مع نظام التشغيل .
  - ظهور رسائل خطأ غير منطقية .
  - عدم القدرة على تشغيل بعض البرامج .
  - اختفاء بعض الملفات .
  - تغير أسماء بعض الملفات .
  - ظهور ملفات غريبة .
  - تناقص المساحة الخالية على أجزاء القرص الصلب .

- إغلاق الحاسب بشكل تلقائي دون وجود سبب يدعو لذلك .

- التخلص من الفيروس لا يتم إلا عن طريق استخدام برنامج مضاد للفيروسات– مع العلم أن هناك طرق أخرى ، ولكنها تحتاج إلى مستخدم محترف .
- فكرة عمل البرامج المضادة للفيروسات تقوم على وجود مكتبة يطلق عليها اسم **Virus Definition** تحتوي على العديد من أنواع الفيروسات ، ويقوم البرنامج بفحص الملفات الموجودة على الحاسب ومطابقتها بهذه المكتبة للتعرف على وجود فيروس أم لا .
- يجب دائما تحديث مكتبة **Virus definition** لزيادة قدرة البرامج المضادة للفيروسات للتعرف على الأنواع الجديدة .
- من أكثر البرامج التي يمكن الاعتماد عليها برنامج **Norton** بإصداراته المختلفة .
- بغرض النظر عن إصدار **Norton** الذي تستخدمه ، فإنه يمكنك الاطمئنان إلى هذا البرنامج طالما أنك تقوم بتحديثه بشكل دوري .
- يتميز برنامج **Norton** عن غيره من البرامج بأنه يحتوي على العديد من المزايا التي تجعل من استخدامه أمر ضروري ، ومن أهم هذه المزايا أنه برنامج مجاني ، كما أن

الشركة المنتجة لا تتقاضى أية مصاريف مقابل عملية التحديث .

- هناك العديد من البرامج المضادة للفيروسات التي يمكن الحصول عليها من خلال شبكة الإنترنت ، ولكنك إذا ذهبت وراء البحث عن أفضل هذه البرامج فإنك سوف تقضي أوقاتا طويلة في البحث والتدقيق دون الحصول على نتيجة حاسمة .
- هناك بعض المعايير التي يجب تطبيقها لتحديد أفضل البرامج المضادة للفيروسات تتمثل في الآتي :
  - أن يكون البرنامج مجاني .
  - أن يكون قادر على اكتشاف الفيروسات أثناء نقل البيانات أو أثناء الحصول على بيانات من خلال الإنترنت .
  - أن تقوم الشركة المنتجة بتحديث مكتبة الفيروسات خلال فترات قصيرة لتلافي الإصابة بالفيروس .
- إذا قمت بتطبيق المعايير السابقة ، فسوف تجد أنها جميعا موجودة في برنامج **Norton** .
- إذا كنت تحتفظ ببعض البيانات الهامة التي تخشى عليها من الإصابة بالفيروس ، فإن أفضل طريقة لتأمين هذه البيانات هو ضغطها باستخدام أحد برامج الضغط مثل **WinZip** ، **WinRar** ، **Win Ace** [وهو أفضلهم] .
- لا يصيب الفيروس عادة ملفات الأفلام أو الأغاني لأنها تتميز بتشفير عالي يصعب على الفيروس اختراقه .

- ينصب تركيز الفيروس في معظم الأحيان على إصابة الملفات التنفيذية لأنها الملفات الأكثر استخداما ، بالإضافة إلى سهولة إصابتها .

الفصل الثامن

الإختراق

الفصل الثامن

الاختراق



كيف تواجه عدوا لا تعرف عنه شيئا ؟

سؤال بسيط ، لكنه في صميم الموضوع ...

إذ كيف يمكنك التصدي لعدو لا تعرف عنه أو عن الأساليب التي يستخدمها إلا بعض المعلومات التي سمعتها من أصدقاءك عن قدراتهم الفائقة في استخدام برامج الاختراق – والتي تكون عادة من نسيج الخيال !!

إذا الخطوة الأولي للتصدي لهذا العدو هو معرفة الأساليب التي يستخدمها في عملية الاختراق .



هل أفهم من ذلك أن هذا الجزء من الكتاب سوف يتناول كيفية اختراق الأجهزة ؟

لا .. لا أستطيع القيام بذلك ، ولكني سوف أجعلك **harmless hacker** . فموضوع الاختراق اعقد مما تتصوره ، فالاختراق الناجح – بكل ما تعنيه كلمة النجاح من معني – يحتاج إلى وقت كبير للتخطيط والتدبير ، وعادة ما يمكن اكتشاف الجاني بسهولة عن طريق تتبعه .

أضف إلى ذلك أن عملية الاختراق عادة ما تفشل ، لأنه كما يوجد برامج للاختراق ، يوجد برامج للتأمين ضد عمليات الاختراق .. وكلاهما متاح ويمكن الحصول عليه بسهولة .

فعندما حاولت الحصول على بعض برامج الاختراق بهدف شرحها داخل هذا الكتاب ، كل ما تتطلبه الأمر هو قضاء ساعة واحدة على شبكة الإنترنت للبحث عن هذه البرامج – المجانية – وإجادتها !!

ولهذا اعتقد أن عملية الاختراق الناجحة تأتي إما عن طريق خطأ المستخدم ذاته ، أو عن طريق ضربة حظ .

إذا ، ارجوا منك أن تنسى كل ما تعرفه من أساطير حول موضوع الاختراق **Hacking** ولنحاول معا خلال الفصول التالية أن ندرس هذا الموضوع بأسلوب منظم ، لنعرف هذا الخطر الذي يهدد تكنولوجيا المعلومات .

وقبل أن نبدأ ، أحب أن أوضح مرة أخرى أن هذا الكتاب ليس الغرض منه هو تعليم برامج الاختراق ، وأن البرامج التي سوف يتم تناولها لا يمكن استخدامها في عمليات الاختراق الاحترافية التي نسمع عنها ، فهذه البرامج – التي نحن بصدد شرحها – يمكن اكتشافها بسهولة من قبل أي مستخدم ...

إن عملية الاختراق تعني التسلل إلى البيانات الموجودة على حاسب آخر دون علم صاحبها ، وذلك إما لأغراض التخريب أو التجسس .

إذا عملية الاختراق تنقسم إلى شقين ...

الأول : التسلل إلى أحد الأجهزة دون علم صاحبها – الضحية – وهذا التسلل يحتاج بالضرورة إلى أدوات خاصة .

الثاني : ويأتي بعد نجاح عملية التسلل ، ويتمثل في تخريب الحاسب الذي تم التسلل إليه ، أو التجسس على المعلومات المخزنة به.

التسلل :

اختراق جهاز الضحية والتسلل إليه دون علمه يحتاج إلى مجموعة من الأدوات الخاصة . وهذه الأدوات يمكن أن تكون بعض البرامج التي تأتي مع نظم التشغيل نفسها مثل برنامج **Telnet** أو برنامج **Ftp** ، وهي برامج تحتاج إلى خبرة خاصة في التعامل معها . أو يمكن أن تكون بعض البرامج التي صممت خصيصا من أجل تسهيل عمليات الاختراق وتلافي استخدام العديد من الأوامر المعقدة .

إذا ، عملية التسلل يمكن تقسيمها إلى شقين ..

الأول : استخدام البرامج الموجودة داخل نظم التشغيل ، ولكنها تحتاج إلى خبرة خاصة كما ذكرنا .

الثاني : استخدام البرامج المعدة خصيصا لأعمال التسلل ، وتتميز هذه البرامج بسهولة الاستخدام .

ملحوظة هامة ...

لأغراض الشرح داخل هذا الكتاب ، فإن جميع الأمثلة التي سوف نستعرضها قد تم تطبيقها على أحد الأجهزة المرتبطة بشبكة داخليه . ولكنه الأمر لا يختلف عن الاختراق عبر شبكة الإنترنت .

التسلل عن طريق نظم التشغيل :

من المعروف أن نظم التشغيل مليئة بالثغرات التي يمكن استخدامها في عمليات التسلل والاختراق ، ولكن الأمر الذي لا يعرفه الكثير أن البرامج التي تستخدم في عمليات التسلل لا تمثل ثغرات في نظم التشغيل ، وإنما هي عبارة عن بروتوكولات يستخدمها النظام للتعامل مع شبكة الإنترنت أو الشبكات الداخلية بأنواعها .

ما المقصود بالبروتوكولات ؟

من المعروف أن فكرة الشبكات – سواء الداخلية أو شبكة الإنترنت- تقوم على ربط أكثر من حاسب ببعض لتبادل البيانات .
والآن تخيل معي انك تستخدم نظام **Windows98** ، وحاسب آخر مثبت عليه نظام **Unix** ، وثالث مثبت عليه نظام **NT** ، فكيف يمكن في هذه الحالة تبادل البيانات عبر هذه النظم المختلفة ؟
إذا ، يحتاج الأمر هنا إلى سياسة أو بروتوكول خاص يمكن عن طريقه تبادل البيانات بين الحاسبات المختلفة بغض النظر عن نظم التشغيل التي تستخدمها.
إذا البروتوكول يعني ببساطة نظام خاص لتنظيم تبادل البيانات داخل الشبكة.

وهناك العديد من البرامج أو البروتوكولات الموجودة داخل نظم التشغيل ، والتي يمكن من خلالها القيام بعمليات الاختراق ، منها **Telnet** ، **Ftp** .

والآن ، سوف نعطي مثالا لكيفية استخدام بعض هذه البرامج في القيام بعمليات التسلل ..

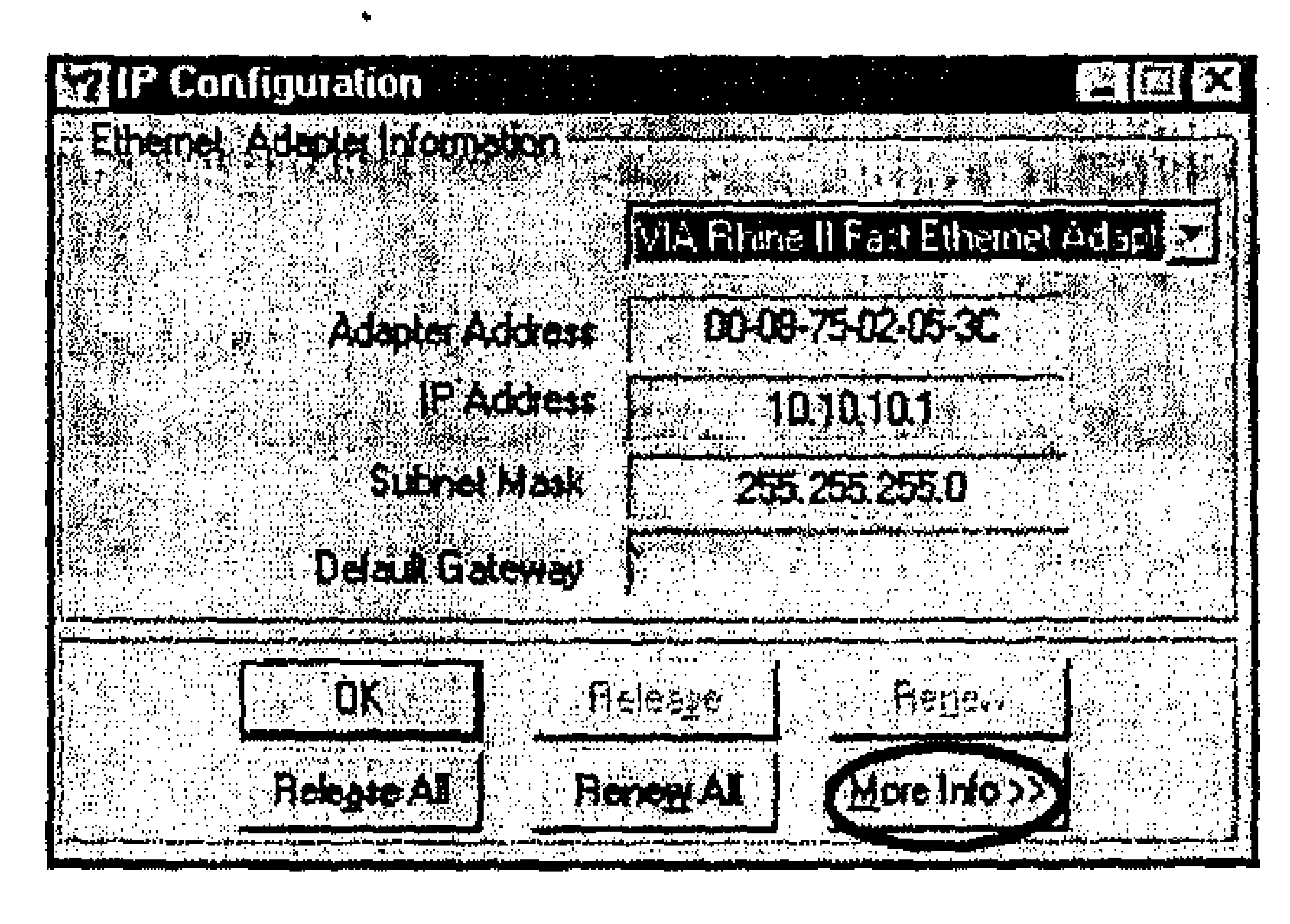
الخطوة الأولي - البحث عن الضحية :

البحث عن الضحية يكون عن طريق معرفة رقم **IP** الخاص به ..

ما المقصود برقم IP ؟
إذا كان الحاسب الخاص بك متصلا بشبكة داخلية أو بشبكة الإنترنت ، فإنه يأخذ رقما خاصا لتمييز هذا الحاسب عن باقي الأجهزة المتصلة بالشبكة . ويتكون هذا الرقم من أربعة أجزاء ، وكل جزء يتكون من ثلاثة أرقام كحد أقصى كالتالي : **216.239.33.1**

فيمكنك بسهولة معرفة رقم **IP** الخاص بأحد الأجهزة عن طريق الخطوات التالية ..

1. من القائمة **Start** انتقل إلى العنصر **Run** .
2. داخل النافذة **Run** اكتب الأمر التالي **winipcfg** ، ثم



اضغط مفتاح **Enter** . فتظهر نافذة على الشكل المقابل :

3. وعند الضغط على مفتاح **info More** ، سوف يتغير شكل هذه النافذة ليصبح كالتالي :

IP Configuration
Host Information
Host Name: JIT1
DNS Servers
Node Type: Broadcast
NetBIOS Scope Id
IP Routing Enabled — WINS Proxy Enabled
NetBIOS Resolution Uses DNS
Ethernet Adapter Information
VIA Rhine II Fast Ethernet Adapt
Adapter Address: 00-08-75-02-05-3C
IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
Default Gateway
DHCP Server
Primary WINS Server
Secondary WINS Server
Lease Obtained
Lease Expires
OK | Release | Renew | Release All | Renew All

والذي يعنينا في هذه النافذة هي البيانات الخاصة بـ **Host name** ، **IP address** . حيث أن **Host name** هو عبارة أن اسم الحاسب ، وهذا الاسم يمكن ترجمته للحصول على رقم **IP** الخاص بالجهاز ، أي أنه يحل محل رقم **IP** .



هل يعني ذلك أنه يجب أن أجلس على جهاز الضحية لمعرفة رقم IP الخاص به ؟

كلا ، هناك طريقة أخرى لمعرفة رقم IP الخاص بجهاز الضحية . ولكن هذه الطريقة تتطلب أن تكون متصلا بهذا الجهاز إما عن طريق شبكة الإنترنت ، أو عن طريق شبكة داخلية . فيمكنك معرفة جميع أرقام IP المتصلة بجهازك حاليا عن طريق تنفيذ الخطوات التالية :

1. من القائمة **Start** ، اختر العنصر **Run** .
2. داخل النافذة **Run** ، اكتب الأمر **Command** ، ثم اضغط مفتاح **Enter** ، لتظهر النافذة الخاصة بنظام **Dos** .
3. داخل هذه النافذة ، اكتب الأمر التالي :

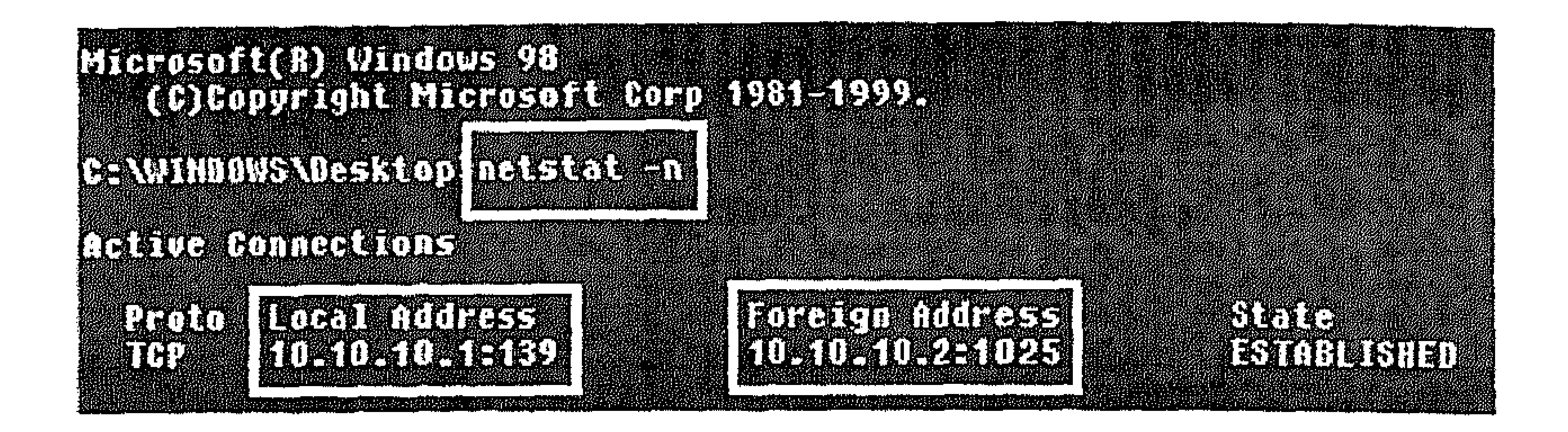
```
C:\windows\Desktop\> Netstat ▽ –n ↵
```

ثم اضغط مفتاح **Enter**

ملحوظة هامة ...

لأغراض التبسيط ، سوف نرمز لمفتاح المسطرة **Space** بالرمز ▽ ، ومفتاح **Enter** بالرمز ↵
بالإضافة إلى أننا بدلا من كتابة عبارة مثل (من القائمة **Start** اختر الأمر **Run** ، ثم اكتب كلمة **Command**) فإننا سوف نشير إليها كالتالي :
Start > Run > Command

فتظهر نافذة كما في الشكل التالي :


```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS\Desktop>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.10.1:139         10.10.10.2:1025        ESTABLISHED
```

فكما يظهر بالشكل ، فإن Local address تشير إلى الحاسب الخاص بك ، حيث يظهر رقم IP بالإضافة إلى رقم Port المستخدم حاليا .

أما بالنسبة لـ Foreign address فيشير إلى الحاسب الآخر المتصل بك ، ويظهر به أيضا رقم IP ، بالإضافة إلى رقم Port .

ما المقصود بـ Port ؟
كلمة Port تعني المنفذ ، وهو عبارة عن الباب الذي تمر منه البيانات من وإلى الحاسب .. مع العلم أنه لا يوجد باب واحد فقط لكل جهاز ، بل هناك العديد من المنافذ التي يمكن من خلالها تمرير البيانات ، ولكن الرقم الموجود في الشكل السابق يشير إلى المنفذ المستخدم حاليا.

وبالتالي ، فيمكنك عن طريق الأمر netstat معرفة أرقام IP المتصلة حاليا بجهازك .

الخطوة الثانية – تحديد مدى القابلية للاختراق :

بعد تحديد الضحية عن طريق معرفة رقم IP ، تأتي الخطوة الثانية التي تتمثل في تحديد إمكانية اختراق جهاز الضحية . فمجرد حصولك على رقم IP لا يعني مطلقا أنك مؤهل لاختراق هذا الجهاز .

ولتحديد مدى قابلية الجهاز للاختراق ، اتبع الخطوات التالية :

1. من قائمة البداية **Start > Run > Command** .
2. اكتب الأمر التالي :

C:\windows\Desktop > nbtstat ▽ -a ▽ 10.10.10.2 ↵

حيث أن الرقم **10.10.10.2** هو رقم **IP** الخاص بجهاز الضحية ..

وبالطبع سوف تقوم باستبداله .

والآن ، أنظر معي إلى الشكل التالي :

```
C:\WINDOWS\Desktop>nbtstat -a 10.10.10.2

       NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
JIT2           <00>  UNIQUE      Registered
JIT            <00>  GROUP       Registered
JIT2           <03>  UNIQUE      Registered
JIT2     -->   <20>  UNIQUE      Registered
JIT            <1E>  GROUP       Registered
JIT            <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered

MAC Address = 00-80-AD-74-E0-5D
C:\WINDOWS\Desktop>_
```



هل تلاحظ هذا الرقم الذي أمامه سهم ؟

إن هذا الرمز هو الكنز الذي يبحث عنه أي مخترق ، فهذا الرمز

<20> يشير ببساطة أن الحاسب JIT2 قد تم تفعيل خاصية File and Print Sharing به ، مما يعني أنه يمكن التجسس على الملفات الموجودة داخل هذا الحاسب ، أو زرع ملفات بداخله .

الخطوة الثالثة – تحديد الأماكن التي يمكن اختراقها :

إن تفعيل خاصية File and Print Sharing تعني أن الضحية قد قام بالسماح للمستخدمين الآخرين بالدخول إلى أماكن محددة داخل الحاسب الخاص به ، مما يعني أنه تبقى خطوة واحدة قبل القيام بعملية الاختراق ، وهي بالطبع تحديد الأماكن التي يمكن اختراقها داخل هذا الحاسب .

ولتحديد هذه الأماكن ، اتبع الخطوات التالية :

1. من قائمة البداية Start > Run > Command .
2. اكتب الأمر التالي :

```
C:\Windows \ Desktop > net ▽view ▽\\10.10.10.2 ↵
```

حيث أن الأمر Net View يستخدم لتحديد الأماكن التي قام الضحية بالسماح بمشاركتها داخل الجهاز .

```
C:\WINDOWS\Desktop>net view \\10.10.10.2
Shared resources at \\10.10.10.2

Sharename      Type          Comment
-------------------------------------------
A              Disk
C              Disk
D              Disk
E              Disk
F              Disk
G              Disk
H              Disk
MY DOCUMENTS   Disk
The command was completed successfully.
```



هل تعلم أن هذا أكثر مما قد يحلم به أي مخترق !!!

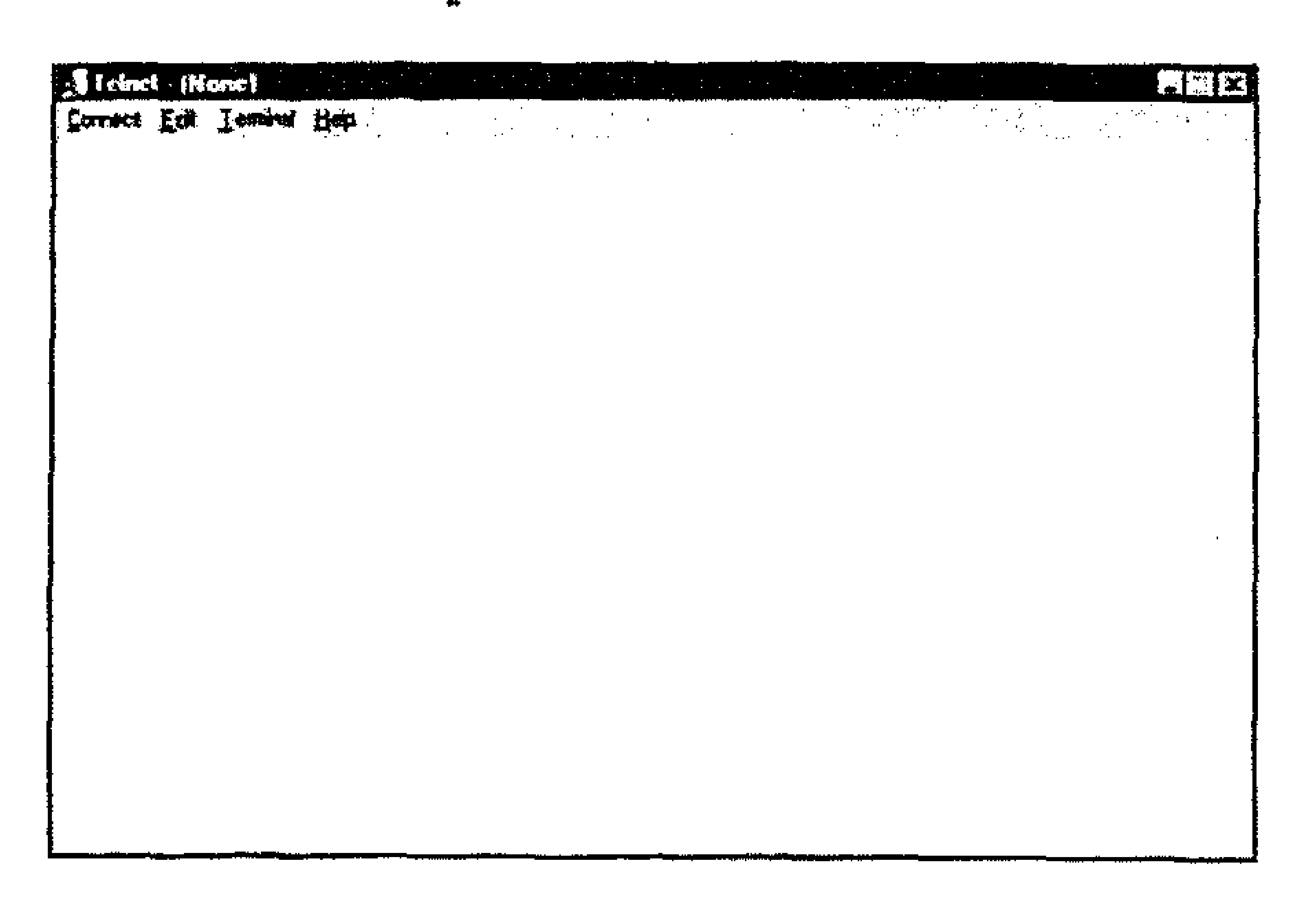
لقد اتضح من خلال تنفيذ الأمر السابق أن الضحية قام بمشاركة وحدة الأقراص المرنة **A** ، بالإضافة إلى الأجزاء من **C** إلى **H** على القرص الصلب ، بالإضافة إلى المجلد **My Document** .. إن الضحية مستعد تماما لتسهيل عملية الاختراق .

الخطوة الرابعة – الاختراق :

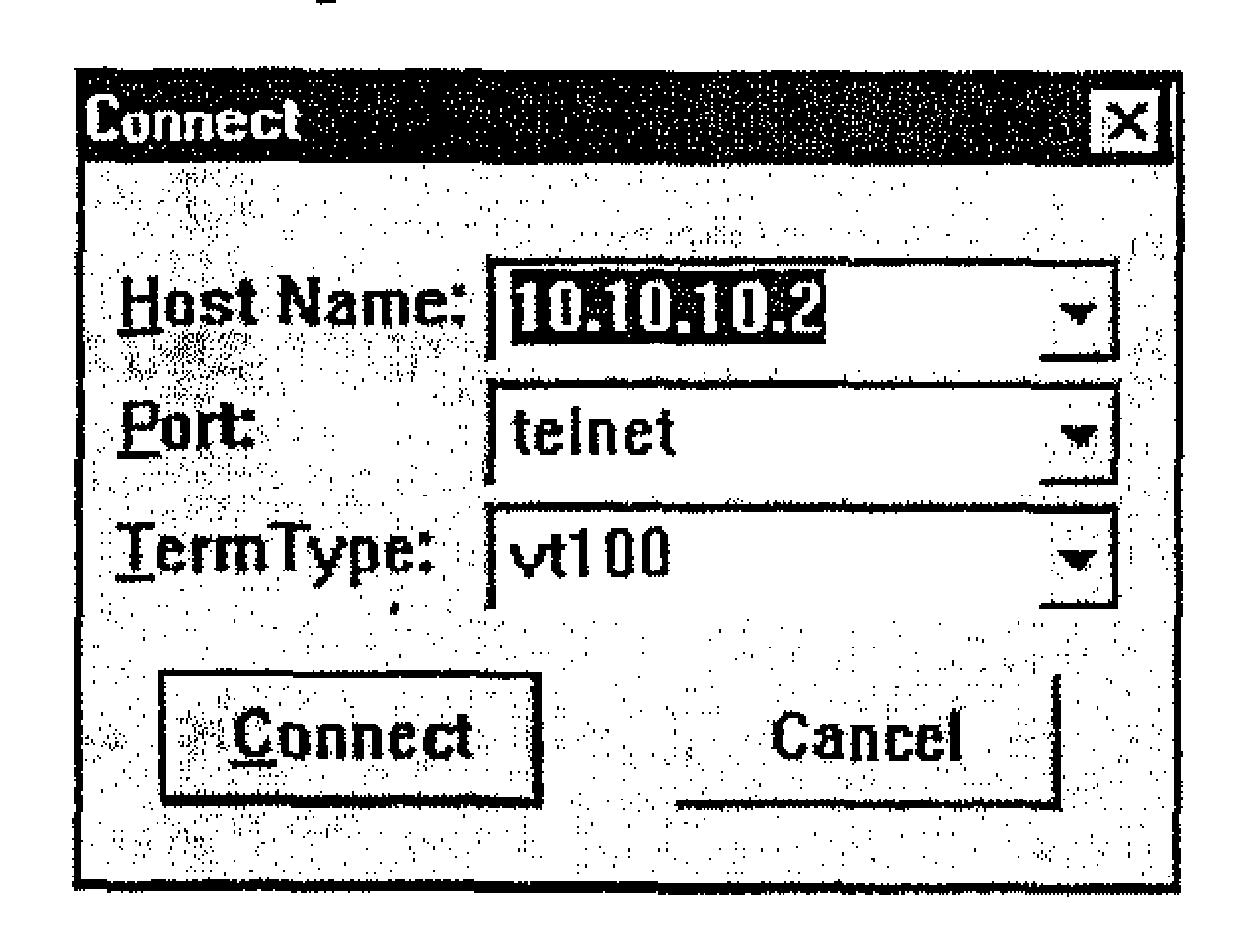
توجد وسيلتين لتنفيذ الاختراق . الوسيلة الأولي تتمثل في استخدام **Telnet** ، أما الوسيلة الثانية فتتمثل في استخدام **FTP** .

الوسيلة الأولي- Telnet :

1. من قائمة البداية **Start > Run > Telnet** .
2. سوف تظهر نافذة على الشكل التالي :



3. اذهب للقائمة **Connect** ، ثم اختر الأمر **Remote system** .
فتظهر نافذة أخرى على الشكل التالي :



4. داخل الحقل **Host name** أدخل رقم **IP** الخاص بجهاز الضحية ، أو **JIT2** وكلاهما يعادل الأخر .. أما بالنسبة لبقية الحقول لا تقوم بتغيير الأوضاع الافتراضية الخاصة بها .
5. اضغط مفتاح **Connect** لتبدأ التحكم في جهاز الضحية .

الوسيلة الثانية – FTP :

الوسيلة الثانية لاختراق جهاز الضحية تتمثل في استخدام البروتوكول FTP ، وهو اختصار لـ **File Transfer Program** ...

هل تقول أنك لا تعرف كيفية استخدام **Telnet** ؟

لقد اتفقنا من البداية أنني سوف أجعلك **Harmless hacker** ، وليس **Professional hacker** .. بالإضافة إلى أن استخدام برنامج **Telnet** يحتاج إلى كتاب مستقل لهذا الموضوع .

هل تعرف ما الذي تستطيع فعله باستخدام **Telnet** ...

- Log into your account on any of the host computers on campus.
- Use the software on those computers.
- Capture data from the screen.
- Transfer files between your computer and the host computer.

والآن ، نعود لموضوعنا حول استخدام **FTP** في عملية الاختراق .

1. من قائمة البداية **Start > Run > Command**
2. اكتب الأمر التالي :

```
C:\Windows\Desktop> ftp ↵
```

3. سوف يتحول شكل المحث إلى **Ftp >**

4. اكتب رمز علامة الاستفهام لاستعراض الأوامر الخاصة بهذا البرنامج . فيظهر الشكل التالي :

```
C:\WINDOWS\Desktop>ftp
ftp> ?
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp>
```

5. للخروج من هذا البرنامج ، اكتب كلمة **bye** ، ثم اضغط مفتاح **Enter** .

والآن .. هل رأيت معي أن عملية الاختراق يمكن أن تكون بسيطة على الرغم من عدم استخدام أية برامج متخصصة ، مع العلم أن عملية الاختراق سوف تكون أبسط مع استخدام البرامج المعدة لذلك .

الفصل التاسع

التسلل باستخدام البرامج

الفصل التاسع

التسلل باستخدام البرامج

التسلل باستخدام البرامج يحتاج إلى مجموعة من الأدوات . ونظرا لكثرة برامج الاختراق التي يمكن استخدامها ، فقدت رأيت أن أفضل وسيلة لتناول هذا الموضوع سوف تكون عن طريق استخدام برنامج **Sub7 legends** ، وهو أحدث إصدارات برنامج **Sub7** ويمكنه العمل تحت بيئة **Window 98 / ME / XP** .

فهذا البرنامج يحتوي على العديد من الإمكانيات التي تغنيك عن استعمال أي برنامج آخر ، بالإضافة إلى سهولة استخدامه ، وكثرة انتشاره .

فكرة عمل برامج الاختراق :

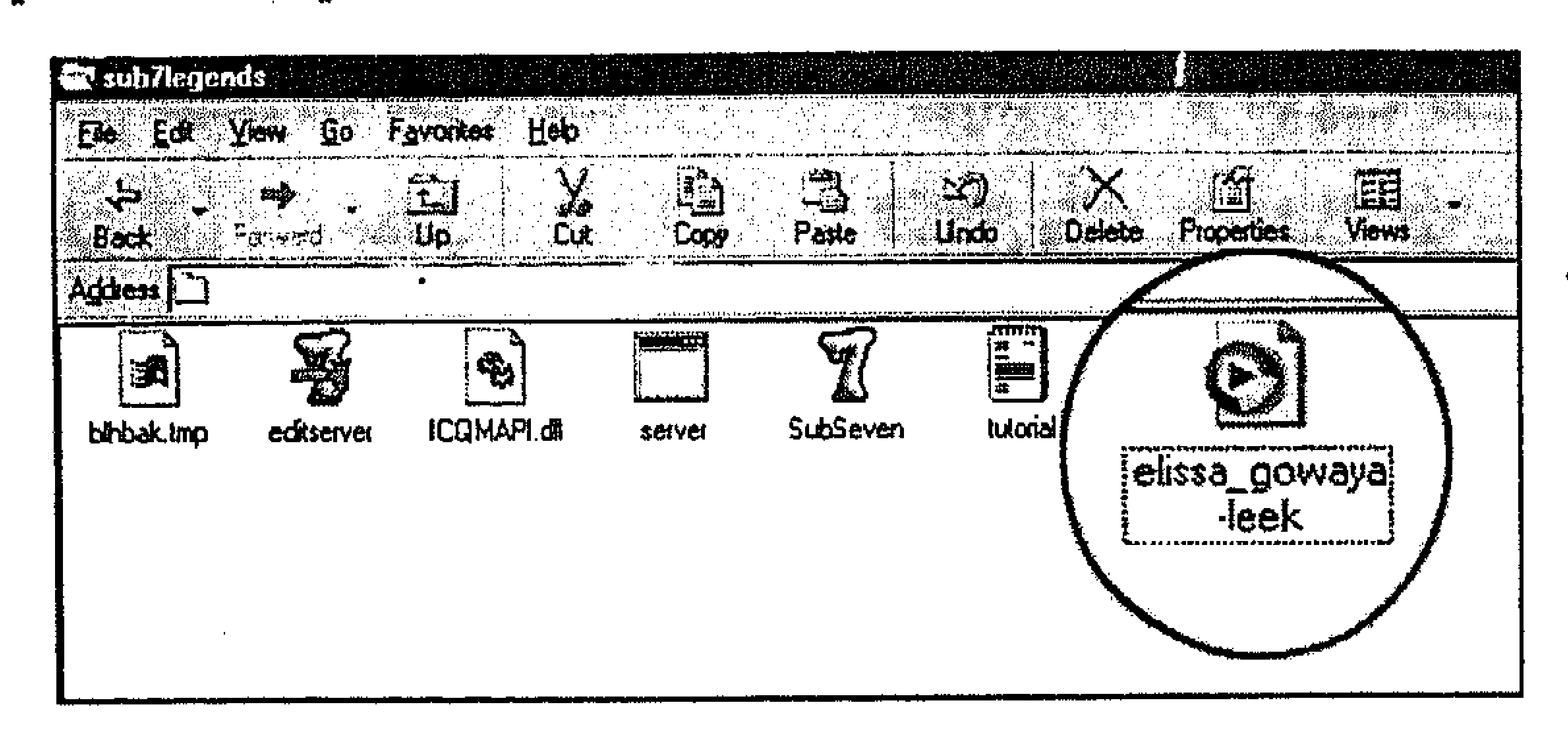
تقوم فكرة عمل معظم برامج الاختراق على زرع **Trojan** داخل جهاز الضحية . وكلمة **Trojan** جاءت من القصة الشهيرة لحصان طروادة ، ولكن هذه الكلمة في مجال الاختراق تعني زرع برنامج صغير داخل جهاز الضحية يمكنك من السيطرة الكاملة على الجهاز . وهذه العملية هي أصعب خطوة في برامج الاختراق .

فعملية زرع الـ **Trojan** داخل جهاز الضحية يجب أن تتم دون علمه ، وبالطبع دون أن يشك في أن هذا الملف سوف يستخدم في أغراض التجسس .

فكل ما يحتاجه المخترق هو أن يقوم الضحية بتشغيل هذا الملف لتتم عملية زرع الـ **Trojan** بنجاح ، حتى وإن قام المستخدم بعد ذلك بإلغاء هذا الملف من الحاسب ، فإن ذلك لا يعني أنه قد تخلص من **Trojan** ، بل يبقى كامنا داخل نظام التشغيل ، ويتم تحميله في كل مرة يتم فيها تشغيل الحاسب .

لذلك ، فإن المخترق دائما ما يلجأ إلى خداع الضحية ليتمكن من زرع هذا الملف الذي يسمى **Trojan** أو **Server** داخل جهاز الضحية .

وتتمثل عملية الخداع في تغيير شكل الأيقونة الخاصة بهذا الملف ، بالإضافة إلى تغيير الامتداد الخاص به ، كما يظهر في الشكل التالي:



فكما يظهر في الشكل ، فإن هذا الملف ما هو إلا **Trojan** الذي سوف يتم إرساله إلى جهاز الضحية ، وبالطبع فإن الضحية لن يشك في مثل هذا الملف عندما يحاول المخترق إرساله .

وبعد أن تتم عملية زرع **Trojan** بنجاح ، فإن عملية الاختراق تصبح من أسهل ما يكون .. فكل ما يتطلبه الأمر هو استخدام برنامج الاختراق للاتصال بملف **Trojan** والتحكم في جهاز الضحية عن طريق الاختيارات الموجودة بالبرنامج .

كيف يتم زرع Trojan :

كما ذكرنا أن زرع **Trojan** هو أصعب ما في عملية الاختراق . فلا يمكن مثلا أن يتم إرسال هذا الملف عن طريق **E-mail** إلى جهاز الضحية ، لأن المواقع التي تقدم خدمة البريد الإلكتروني تقوم بفحص الرسائل ضد وجد الفيروسات ، وملفات **Trojan** يتم قراءتها على أنها فيروس .. وهذا يعني أن الموقع الذي يقدم خدمة البريد الإلكتروني لن يسمح لمستقبل الرسالة – الضحية – بالحصول على هذا الملف ، أو على الأقل سوف يقوم بتحذيره . ولن ينجح هذا الأسلوب إلا إذا كان الضحية يستخدم برنامج **Outlook Express** للتعامل مع البريد الإلكتروني . لأن استخدام هذا البرنامج يتيح

التعامل مع البريد الإلكتروني دون الدخول على الموقع الـذي يقـدم خدمة البريد الإلكتروني .

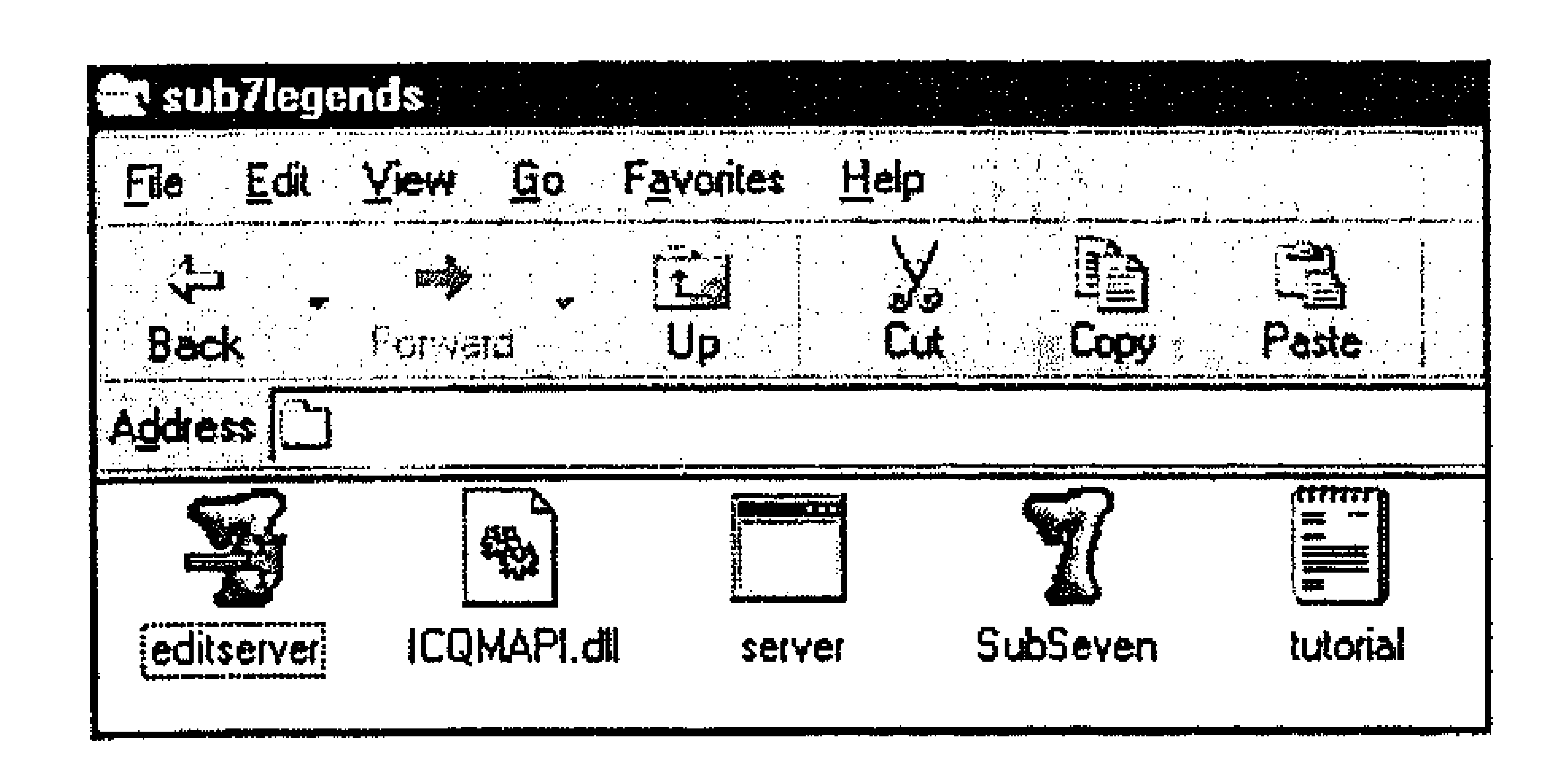
فإذا كنت تملك مثلا بريد إلكتروني داخل موقع **Yahoo** ، فيمكنك عن طريق استخدام برنامج **Outlook Express** أن تقوم بقراءة وإرسـال البريد الإلكتروني دون الدخول على موقع الشركة المقدمة للخدمـة . وهي ثغرة يستغلها العديد من **Hackers** .

إذا ، عملية زرع **Trojan** لا تتم عن طريق إرسـال الملـف إلـى الضحية عن طريق البريد الإلكتروني .. وإنما عادة ما تتم عن طريق إرسال هذا الملف إلى الضحية مباشرة أثناء القيـام بالدردشـة مـع الضحية عن طريق إحدى بـرامج الدردشـة مثـل **ICQ** ، **MSN** ، **Yahoo messenger** ، **MIRC** . لأن هذه العملية تضمن عدم فحص ملف **Trojan** أثناء إرساله ، إلا إذا كان الضحية يستخدم أحد البرامج المضادة للاختراق مثـل برنـامج **Zone Alarm** أو أحـد البـرامج المضادة للفيروسات مثل **Norton** .

تجهيز Trojan :

عند الحصول، على نسخة من برنامج **Sub7** ، فإن هذه النسخة تكون مضغوطة في شكل **Zip Archive** . وعند فك هذه النسخة ، سـوف

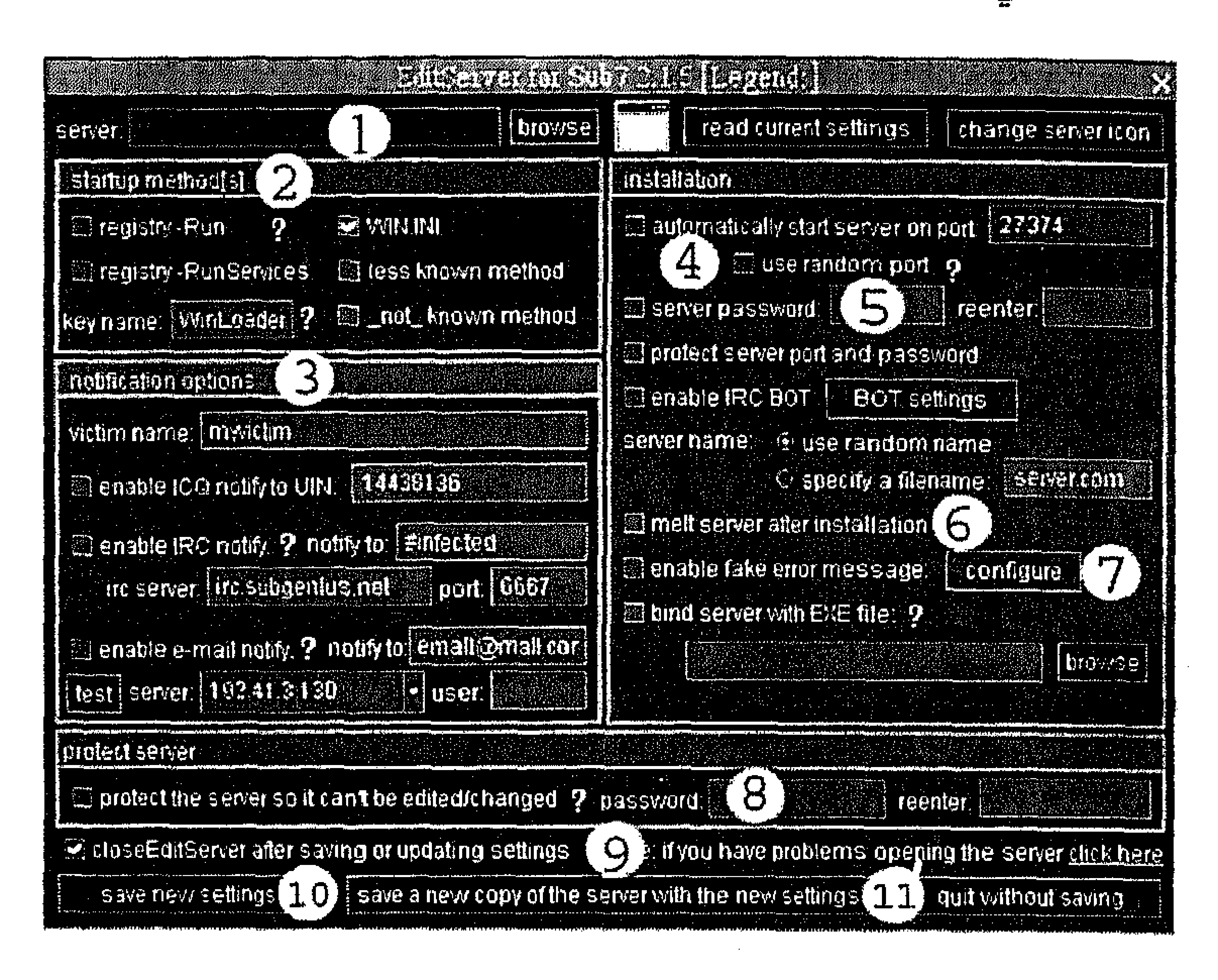
يتم إنشاء مجلد يحمل نفس اسم النسخة المضغوطة يحتوي على خمسة ملفات أساسية ، كما يظهر في الشكل التالي :



EditServer	البرنامج الذي يستخدم في تجهيز Trojan وضبط خصائصه .
ICQMAPI.dll	ملف خاص بالتحكم في برنامج ICQ .
Server	ملف Trojan . ويجب مراعاة عدم تشغيل هذا الملف ، لأنه إذا قمت بتشغيله فإن ذلك يعني أنك قمت بزرع Trojan داخل جهازك .
SubSeven	وهو البرنامج الذي يتم من خلاله التحكم في جهاز الضحية بعد زرع Trojan.
Tutorial	ملف يحتوي على شرح لكيفية استخدام البرنامج ، وكيفية ضبط خصائص ملف Trojan .

ولتجهيز الـ **Trojan** ، اتبع الخطوات التالية :

1. قم بتشغيل برنامج **EditServer** ، لتظهر نافذة على الشكل التالي:



2. قم بإعداد الاختيارات التالية كما يوضحها الجدول :

الرقم	الوظيفة
1	اضغط مفتاح **Brows** ، فتظهر أمامك نافذة **Open** لتقوم بتحديد مكان ملف **Server** ، وهو بالطبع داخل المجلد الخاص بالبرنامج .
2	يحتوي هذا الجزء على مجموعة من الاختيارات الخاصة بكيفية بدأ تشغيل **Trojan** داخل جهاز الضحية . ويفضل التأشير على جميع هذه الاختيارات .. أما بالنسبة للحقل **name Key** فلا تغير قيمته الافتراضية .

الرقم	الوظيفة
3	الجزء **Options Notification** يحتوي على بعض المعلومات مثل اسم الضحية ، كما يمكنك تنشيط الاختيار **Enable ICQ notify to UIN** ، ثم وضع رقم **ICO** الخاص بك ، حتى يقوم برنامج **ICQ** بتنبيهك بمجرد دخول الضحية ، وبالمثل يمكنك تفعيل الاختيار الخاص ببرنامج **IRC** إذا كنت تستخدمه . ويفضل بالطبع عدم كتابة أي معلومات قد ترشد إلى شخصية المخترق.
4	يفضل التأشير أمام الاختيار **Use Random Port** حتى يقوم البرنامج بالتسلل عبر منفذ عشوائي في كل مرة إلى جهاز الضحية.
5	يستخدم الاختيار **Server Password** لحماية ملف **Trojan** من تسلل أي مخترق آخر يستخدم برنامج **Sub7** إلى جهاز الضحية الخاص بك ، وإذا لم يقوم المخترق بحماية **Trojan** فإن هذا يعني أن أي مخترق آخر يستخدم برنامج **Sub7** يستطيع التحكم في جهاز الضحية .
6	إذا قمت بالتأشير أمام هذا الاختيار ، سوف يختفي ملف **Trojan** بمجرد أن يقوم الضحية بتشغيله .. ولكنه سوف يظل يعمل في **Back ground** .
7	إذا أردت أن يصبح ملف **Trojan** أكثر إقناعا وخداعا للضحية ، فيمكنك أن تقوم بتفعيل هذا الاختيار . حيث يعمل هذا الاختيار على عرض رسالة خطأ للضحية عندما يقوم بتشغيل ملف **Trojan** ، مما يجعل الضحية يعتقد أن الملف الذي قمت بإرساله حدث به خطأ أثناء نقله عبر شبكة الإنترنت .

الرقم	الوظيفة
	ويمكنك التحكم في الرسالة التي سوف تظهر للضحية عن طريق الضغط على مفتاح **Configure** .
8	عند التأشير على هذا الاختيار ، فإنك بذلك تضمن حماية ملف **Trojan** ضد أي تعديل يمكن أن يقوم به أي مخترق آخر أو يقوم به الضحية نفسه .
9	هذا الاختيار يكون نشط في الوضع الافتراضي ، حيث يعمل هذا الاختيار على توقف ملف **EditServer** عن العمل بعد أن قمت بتعديل ملف **Trojan** وحفظه .
10	عند الضغط على مفتاح **Save new settings** سوف يتم حفظ التغييرات التي قمت بها داخل ملف **Server** نفسه .
11	عند الضغط على هذا المفتاح سوف يتم حفظ نسخة جديدة من ملف **Trojan** تحتوي على التغييرات الجديدة ، دون التغيير في الملف الأصلي .

وبعد أن يتم ضبط الاختيارات السابقة ، يصبح لديك ملف **Trojan** جاهز لإرساله إلى الضحية .

تحديد الضحية :

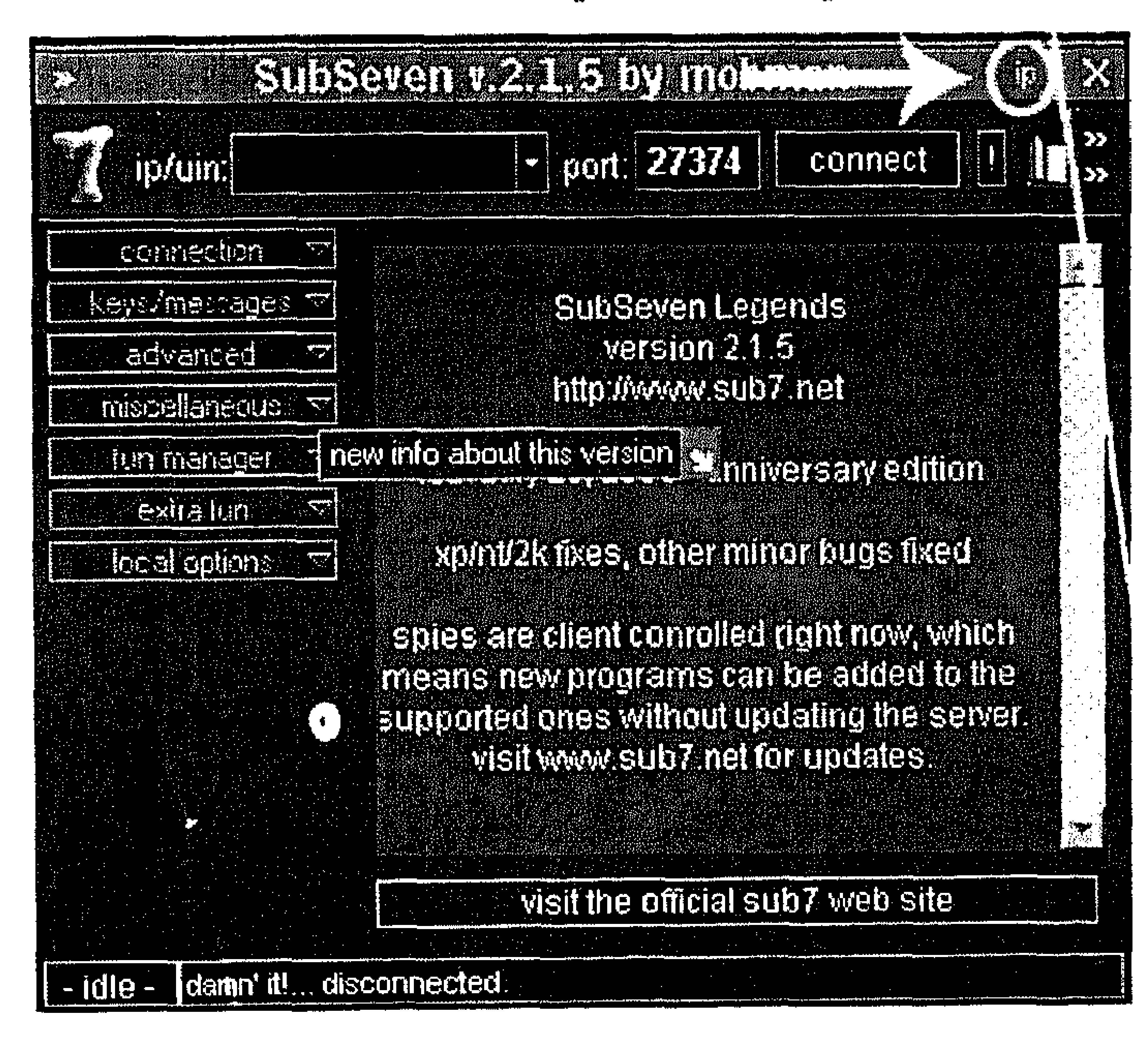
كما رأينا في الفصل السابق أن عملية تحديد الضحية تتم عن طريق معرفة رقم **IP** الخاص به . ويمكن القيام بذلك إما عن طريق رقم

ICQ الخاص بـ ، أو عن طريق عمل مسح عشوائي لنطاق معين من أرقام **IP** لتحديد ما إذا كان هناك جهاز يصلح لأن يكون ضحية .

وعادة ما تكون الضحية شخصا تعرفه أو على الأقل تعرف رقم **ICQ** الخاص به ، لأن الاختيار العشوائي يستغرق أوقاتا طويلة ، كما أن عملية الاختراق لا تصلح عادة مع شخص لا تعرف عنه شيئا على الإطلاق .

ولمعرفة رقم **IP** عن طريق رقم **ICQ** الخاص بالضحية ، يتم القيام بالخطوات التالية :

1. من النافذة الرئيسية لبرنامج **Sub7** ، اضغط فوق كلمة **IP** ، كما يظهر في الشكل التالي :

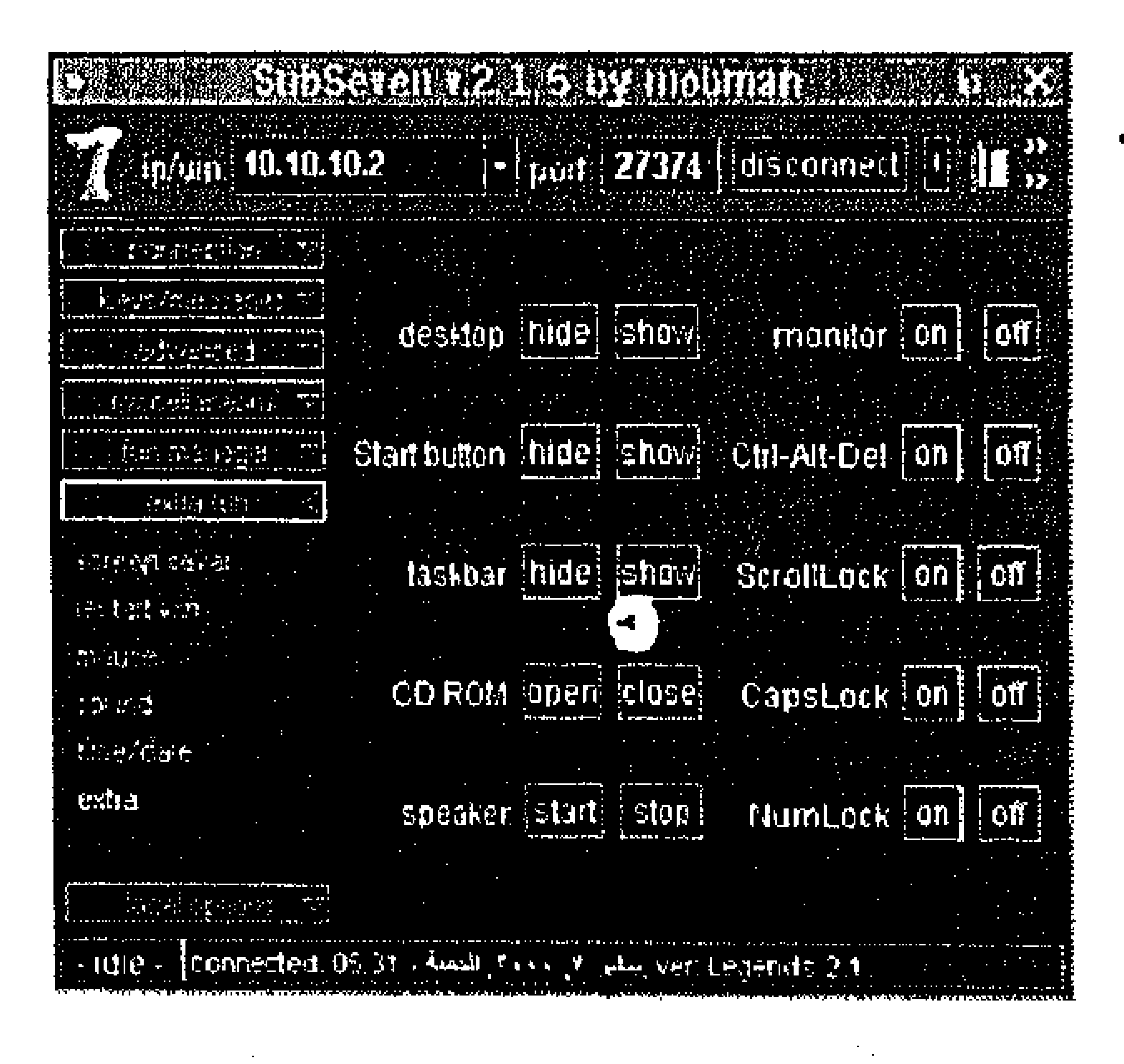


2. سوف تظهر نافذة أخرى على الشكل التالي :

حيث يتم كتابة رقم **ICQ** الخاص بالضحية ، ثم الضغط على مفتاح **Resolve UIN** . وبذلك تحصل على رقم **IP** الخاص بالضحية .

تنفيذ الاختراق :

بعد أن يتم إرسال **Trojan** إلى الضحية ، بالإضافة إلى معرفة رقم **IP** الخاص به ، يصبح الضحية تحت تصرفك الكامل .



فكل ما عليك القيام به هو تشغيل.
برنامج **Sub7** ، ثم داخل الحقل **IP/UIN** أدخل رقم **IP** الخاص ب، ثم اضغط مفتاح **Connect** لتبدأ في التحكم ...



ما هي إمكانيات برنامج Sub7؟

يحتوي هذا البرنامج على العديد من الإمكانيات ، ومن أهمها :

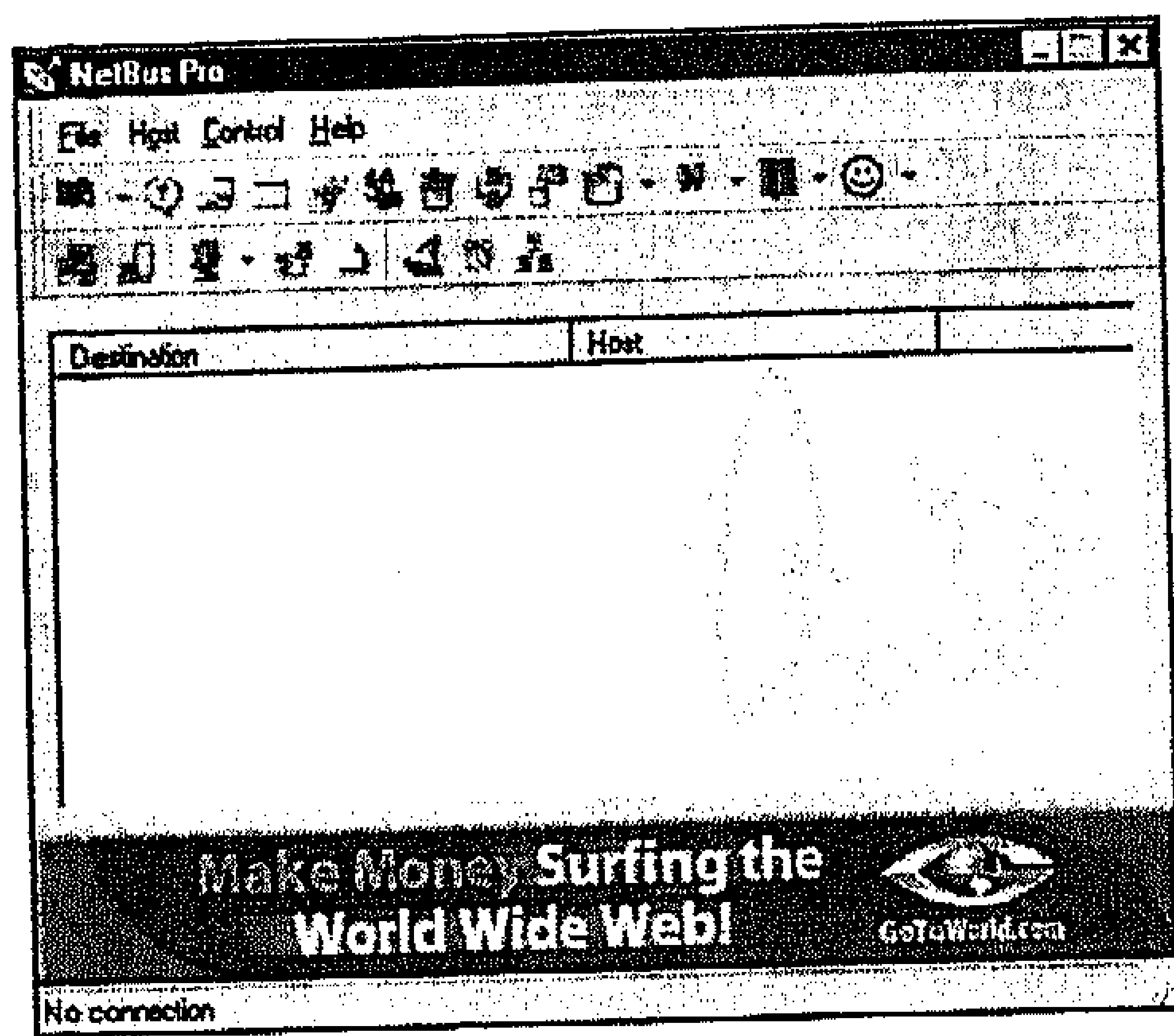
- address book
- WWP Pager Retriever
- UIN2IP
- remote IP scanner
- host lookup
- get Windows CD-KEY
- update victim from URL
- ICQ takeover
- FTP root folder
- retrieve dial-up passwords along with phone numbers
- and usernames
- port redirect
- IRC bot. for a list of commands
- File Manager bookmarks
- make folder, delete folder [empty or full]
- process manager
- text 2 speech
- Restart server
- Aol Instant Messenger Spy
- Yahoo Messenger Spy
- Microsoft Messenger Spy
- Retrieve list of ICQ uins and passwords
- Retrieve list of AIM users and passwords
- App Redirect
- Edit file
- Perform clicks on victim's desktop
- Set/Change Screen Saver settings [Scrolling Marquee]
- Restart Windows.
- Ping server
- Compress/Decompress files before and after transfers

- The Matrix
- Ultra Fast IP scanner
- IP Tool [Resolve Host names/Ping IP addresses]
- Get victim's home info [not possible on all servers]:
  - Address
  - Bussiness name
  - City
  - Company
  - Country
  - Customer type
  - E-Mail
  - Real name
  - State
  - City code
  - Country code
  - Local Phone
  - Zip code

And more...

: NetBus

برنامج NetBus هو أحد برامج Hacking مثل برنامج Sub7 ، ولكن Trojan الخاص به أقدم من برنامج Sub7 .



ويمكن عن طريق هذا البرنامج تنفيذ ما يلي :

- Open/close the CD-ROM once or in intervals (specified in seconds).
- Show optional image. If no full path of the image is given it will look for it in the Patch-directory. The supported image formats is BMP and JPG.
- Swap mouse buttons - the right mouse button gets the left mouse button's functions and vice versa.
- Start optional application.
- Play optional sound-file. If no full path of the sound-file is given it will look for it in the Patch-directory. The supported sound-format is WAV.
- Point the mouse to optional coordinates. You can even navigate the mouse on the target computer with your own.
- Show a message dialog on the screen. The answer is always sent back to you.
- Shutdown the system, logoff the user etc.
- Go to an optional URL within the default web-browser.
- Send keystrokes to the active application on the target computer. The text in the field "Message/text" will be inserted in the application that has focus. ("|" represents enter).
- Listen for keystrokes and send them back to you.
- Get a screen dump (should not be used over slow connections).
- Return information about the target computer.
- Upload any file from you to the target computer. With this feature it will be possible to remotely update Patch with a new version.
- Increase and decrease the sound-volume.
- Record sounds that the microphone catch. The sound is sent back to you.
- Make click sounds every time a key is pressed.
- Download and deletion of any file from the target. You choose which file you wish to download/delete in a view that represents the hard disks on the target.
- Keys (letters) on the keyboard can be disabled.
- Password-protection management.
- Show, kill and focus windows on the system.
- Redirect data on a specified TCP-port to another host and port.
- Redirect console applications I/O to a specified TCP-port (telnet the host at the specified port to interact with the application).
- Configure the server-exe with options like TCP-port and mail notification.

الفصل العاشر

اختراق حسابات البنوك

الفصل العاشر

اختراق حسابات البنوك

كلما ذكرت أمام أحد الأشخاص أن عملية اختراق حسابات البنوك سهله ويمكن القيام بها إذا كنت تملك الأدوات المناسبة . كان الرد عبارة عن علامة تعجب كبيرة !!!

فعلى الرغم مما تبدو عليه هذه العملية من تعقيد ، إلا أنها مبنية على فكرة بسيطة .. فالقيام بهذه العملية يتطلب :

1. معرفة اسم الضحية ، وكلمة السر الخاصة به .
2. معرفة رقم الحساب ، بالإضافة إلى اسم البنك .

والآن ، لنلقي نظرة حول كيفية قيام البنك بتأمين الموقع الخاص به لضمان سرية التعامل مع حسابات العملاء .

إذا كنت تملك حساب في أحد البنوك ، فإنك تعرف أن البنك لا يسمح لك بالتعامل مع الحساب عبر شبكة الإنترنت ، إلا إذا كنت تملك متصفح إنترنت **WEB Explorer** يدعم نظام التشفير **128 Encryption** على الأقل .



هل تعلم ماذا يعني 128 Encryption ؟

كلمة **Encrypt** تعني تشفير ، ولغرض تبسيط المعلومة سوف نعتبر أن هذه الكلمة تعني (قفل) **Lock** .

فإذا افترضنا أن البنك يقوم بتأمين البيانات عن طريق استخدام نظام تشفير **40-bit Encryption** ، فإن هذا يعني أن هناك (2^{40}) احتمال يجيب تجربتهم حتى يمكنك الحصول على المفتاح المناسب .

أما إذا كان البنك يقوم بتأمين البيانات عن طريق استخدام نظام تشفير **128-Bit Encryption** ، فإن هذا يعني أن هناك (2^{88}) احتمال يجب تجربتهم حتى يمكنك الحصول على المفتاح المناسب .



هل تعلم ما هي قيمة (2^{88}) ؟

إنها تساوي (3 يتبعها 26 صفر) ... وهو رقم هائل بالطبع .

وهذا يعني نظريا أنه من غير المحتمل لأي شخص – حتى وإن كان محترفا – أن يقوم باختراق البيانات التي تم تشفيرها بنظام **128-Bit** .

ولكن الأمر الذي يغيب عن ذهن القارئ أن المخترق لا يحاول التسلل إلى موقع البنك والتجسس على العمليات التي تتم بداخله . بل إنه يتجسس على المستخدم نفسه ..

فكل ما يحتاجه المخترق لتنفيذ عملية التسلل هو برنامج صغير يستطيع الحصول على **Key Stroke** من جهاز الضحية ، وهذا يعني

أنه يستطيع أن يعرف ما الذي يقوم الضحية بكتابته عن طريق لوحة المفاتيح ، ويتم تخزين هذه القيم داخل ملف خاص على جهاز الضحية تمهيدا لإرساله إلى المخترق .

ويمكن لملف **Trojan** أن يقوم بهذه الوظيفة بسهولة إذا تم زرعه داخل جهاز الضحية .

كما يحتاج المخترق أيضا إلى صورة **Print Screen** لسطح المكتب الخاص بالضحية أثناء قيامه بالتعامل مع موقع البنك . وبهذا يستطيع معرفة رقم الحساب واسم البنك الخاص بالضحية !!!

وهذا أيضا يمكن تنفيذه عن طريق ملف **Trojan** .

إذا .. في دينا المعلومات الرقمية لا يوجد ما يسمى مستحيلا

والآن ، هل مازلت لا تصدق أنه لا يمكن التجسس على بياناتك ؟

لما لا تقرأ معي السطور التالية ...

تحويل الحاسب إلى وحدة تجسس :

إن ما أقوله ليس قصة لأحد أفلام الخيال العلمي ، بل إنه واقع .

كم منكم لديه **Web Cam** ؟ كم منكم لديه **Microphone** متصل بالحاسب ؟

هناك بعض أنواع **Trojan** التي يمكن زرعها على الحاسب الخاص بك ، والتي يمكن من خلالها أن يقوم المخترق بتشغيل **Web Cam**

الخاص بك لتسجيل ما يحدث في حجرتك وإرسالها إلى المخترق دون أن تعلم !!

وبالمثل ، يمكن لملف **Trojan** أن يقوم بتسجيل الأصوات الموجـــودة في حجرة الضحية عن طريق الميكروفون المتصل بالحاسب .

هل تعلم أن ملف **Trojan** الذي يأتي مع برنامج **Sub7** يستطيع تنفيذ ذلك بسهولة !!!

الفصل الحادى عشر

تأمين البيانات

الفصل الحادي عشر

تأمين البيانات

بعد أن قرأت الفصول السابقة . أريدك أن تجيب على سؤال واحد..
هل دفعتك إلى الشك في مدى إمكانية اختراق جهازك ؟
إذا كنت قد فعلت ذلك ، فقد نجحت في أداء مهمتي !!!
إن الغرض من الفصول السابقة – كما ذكرت من قبل – لا يتمثل في تعليم القرصنة وكيفية اختراق الأجهزة ، وإنما الغرض الحقيقي هو أن تعرف ما يقوم به المخترق وما يستخدمه من أدوات من أجل الوصول إلى جهازك .
الآن ، أنت تعرف العدو الذي أمامك ، وتستطيع أن تتصدى له ..
كما يحتاج الاختراق إلى أدوات ، فإن تأمين جهازك ضد الاختراق يحتاج أيضا إلى أدوات . وتتمثل هذه الأدوات فيما يلي :

الجدران النارية :

برامج الجدران النارية **Firewalls** هي عبارة عن برامج صغيرة يتم تثبيتها داخل النظام بغرض مراقبة المنافذ **Ports** التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنت .

وعن طريق مراقبة هذه المنافذ ، يقوم البرنامج بعرض رسائل للمستخدم تفيد بأن هناك موقع معين يحاول كتابة بعض المعلومات داخل جهازك ، أو أن هناك موقع معين يحاول الحصول على بعض البيانات الموجودة داخل جهازك ، فهل تسمح بحدوث ذلك أم لا ؟

ومن أشهر برامج الجدران النارية برنامج **Zone Alarm** ، وهو برنامج مجاني يمكن الحصول عليه من خلال شبكة الإنترنت .

وعلى الرغم من أن مثل هذه البرامج تسبب إزعاجا في بعض الأحيان نتيجة لاستمرار عرض الرسائل ، إلا أنها تضمن حماية وتأمين الجهاز .

وهناك أيضا برنامج **Black Ice Defender** ، وهو برنامج رائع يقوم بمراقبة جميع المنافذ والتصدي لهجمات الاختراق ، كما أنه يقوم بإعطائك العديد من المعلومات حول المتسلل الذي يحاول اختراق جهازك . ويمكنك الحصول على هذا البرنامج من موقع **www.networkice.com** .

كما يمكنك الاستعانة ببرنامج **Lockdown 2000** ، وهو يقوم بنفس الوظائف السابقة ، بالإضافة إلى إمكانية فحص النظام للبحث عن **Trojan** .

ملحوظة هامة ..

أثناء التعامل مع بعض المواقع على شبكة الإنترنت مثل موقع **Yahoo** ، سوف تلاحظ أن هذا الموقع يقوم بتسجيل ملف على الحاسب الخاص بك يتم تخزينه داخل مجلد يطلق عليه **Cookies** داخل مجلد نظام التشغيل . وهذا الملف يحتوي على بعض المعلومات مثل متى قمت بالدخول إلى

الموقع ، والوصلات **Links** التي قمت باستعراضها داخل الموقع ، ووقت الخروج ... الخ.
وفي هذه الحالة سوف يقوم برنامج **Firewall** باعتبار هذا الملف محاولة تسلل إلى الحاسب ، وبالتالي سوف يقوم بعرض رسالة تفيد بأن موقع **yahoo** يحاول التسلل إلى حاسبك ، فهل توافق على ذلك أم لا ؟
إذا ، ليس كل ما يقوم برنامج **Firewall** بعرضه من رسائل يمثل محاولة اختراق للحاسب . وهذا يعني أن رد فعلك يجب يعتمد على من يحاول التسلل إلي حاسبك .

البرامج المضادة للفيروسات :

من أدوات التأمين الهامة ضد عمليات الاختراق والتسلل ؛ برامج مضادات الفيروسات . فبعد التطور الكبير في مجال الاختراق ، قامت الشركات المنتجة لبرامج **Anti Virus** بتوسيع نطاق عملها ليشمل التصدي لعمليات الاختراق ، بالإضافة إلى استخدامها الأساسي للتصدي لفيروسات الحاسب .

فبرنامج **Norton** مثلا يستطيع التعرف على ملف **Trojan** الخاص ببرنامج **Sub7** والتخلص منه بسهولة ، بالإضافة إلى التعرف على العديد من أنواع ملف **Trojan** الأخرى .

كما قامت شركة **Norton** بإضافة إمكانية أخرى لبرامجها أطلقت عليها اسم **Blood Hound** ، حيث تستطيع هذه الوظيفة أن تقوم بعمل حجر صحي **Quarantine** للملفات التي تشك في احتمال إصابتها بالفيروس أو الملفات التي يحتمل أن تكون **Trojan** . ويمكنك بعد ذلك أن تقوم بحذف هذه الملفات أو حتى إرسالها إلى شركة **Norton** نفسها لتقوم بفحصها .

إذا تأمين الحاسب ضد مخاطر الاختراق يعتمد على استخدام كلا من برامج **Firewalls** بالإضافة إلى برامج **Anti Virus** معا .

الفصل الثانى عشر

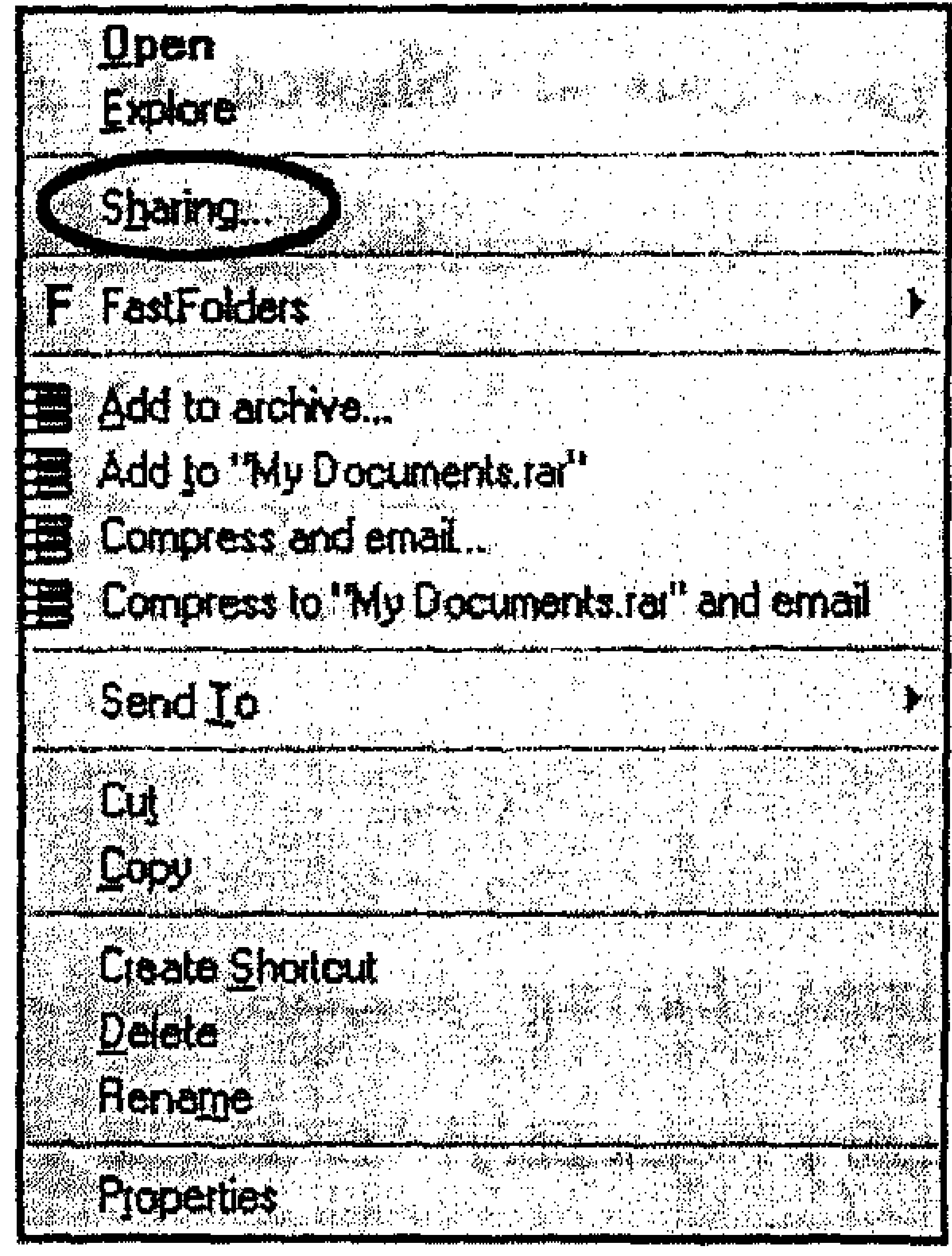
Tips & Tricks

الفصل الثاني عشر
Tips & Tricks

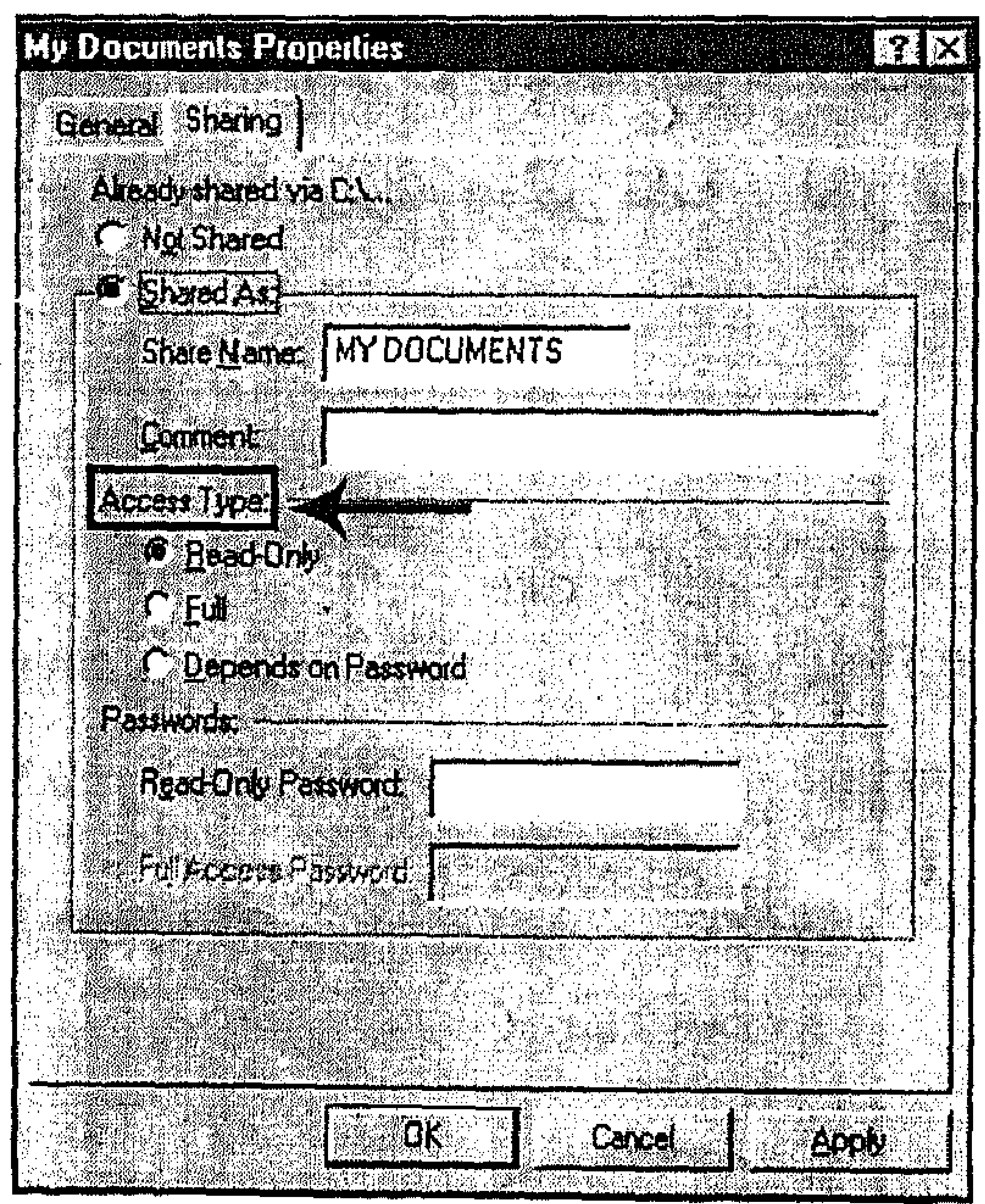
هناك بعض النصائح الأساسية التي أحب أن تنتبه إليها لتأمين الحاسب ضد مخاطر الاختراق ...

1. إذا كنت تتصل بالإنترنت عن طريق **Modem** عادي ، فسوف تلاحظ ظهور أيقونة في الجزء الأيمن من شريط المهام **Task bar** تعطي إشارات معينة تدل على أنك تقوم بإرسال أو استقبال بيانات . وفي هذه الحالة يجب عليك أن تقوم بملاحظة الإشارات الخاصة بهذه الأيقونة . فإذا كنت تقوم باستعراض أحد المواقع واستمرت هذه الأيقونة في الإضاءة ، فإن ذلك قد يعني احتمال وجود تسلل .. إذا يجب عليك أن تقوم بمراقبة هذه الأيقونة .
2. إذا كنت تقوم بتنشيط اختيار **Share** لأحد المجلدات أو أجزاء القرص الصلب ، فيجب عليك أن تقوم بحماية هذه المجلدات بكلمة سر . وذلك عن طريق الخطوات التالية :

أ. أضغط بالمفتاح الأيمن للماوس على أسم المجلد ، فتظهر قائمة على الشكل التالي :



ب. اضغط الأمر **Sharing** ، فتظهر قائمة على الشكل التالي :



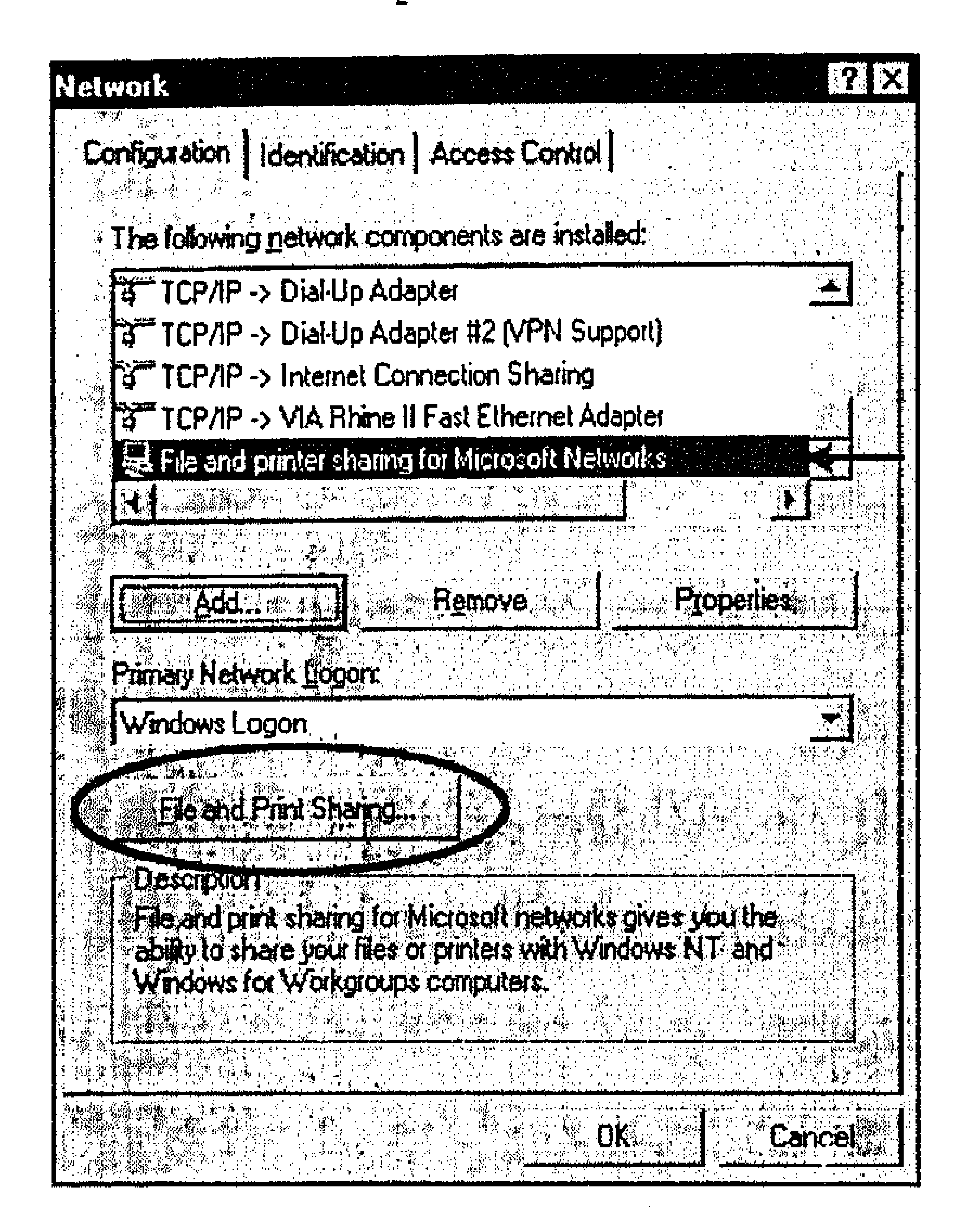
ج. اضغط الاختيار **Shared As** ، ثم انتقل إلـــى الجـــزء **Access Type** الذي يحتوي على الاختيارات التالية :

- **Read Only** : مشاركة للقراءة فقط .
- **Full** : مشاركة كاملة ، ويمكنك حماية هذه المشاركة بكلمة سر .

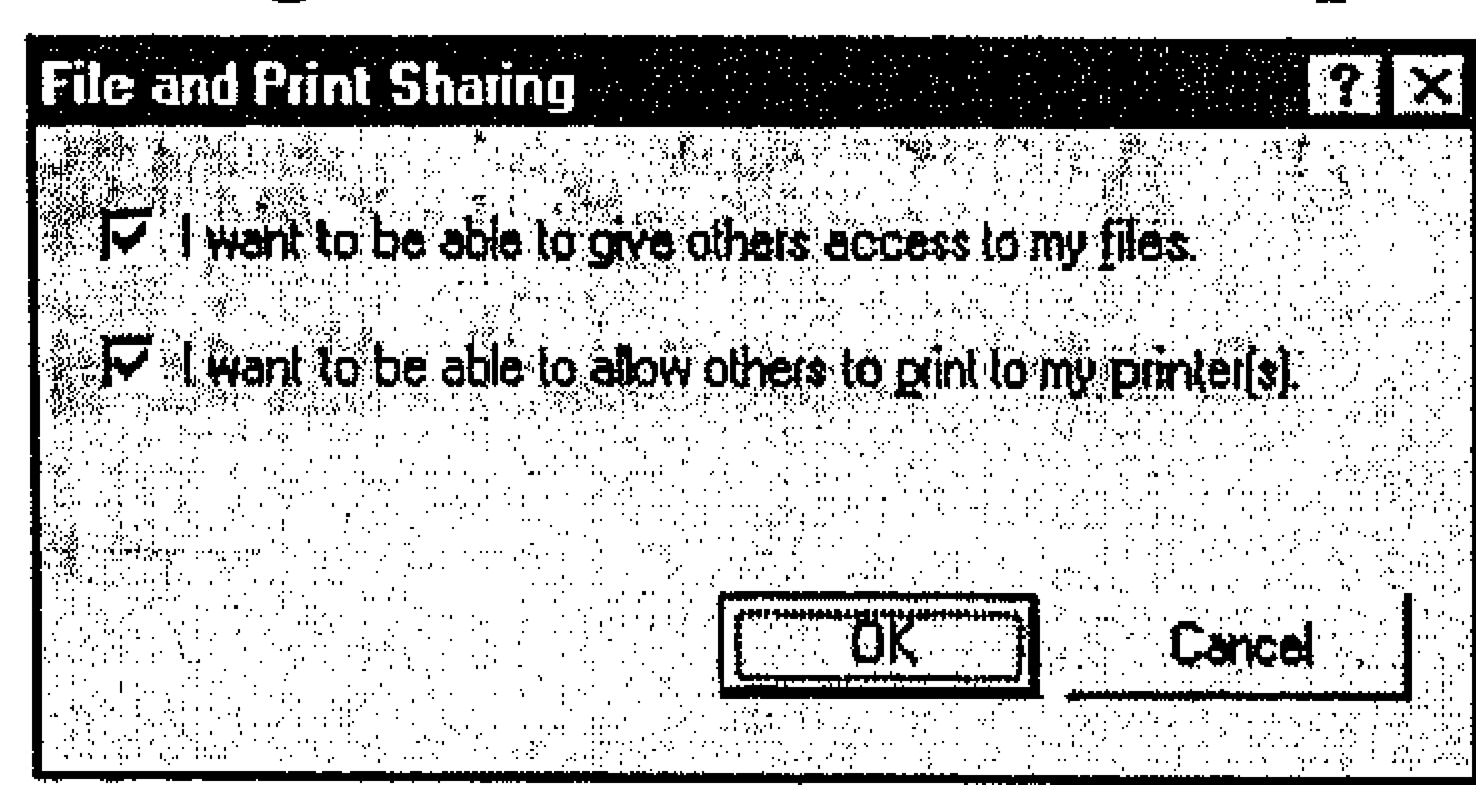
3. إذا كنت لا تســـتخدم الاختيـــار **File and print sharing** فمـــن الأفضل ألا تقوم بتنشيط هذا الاختيـــار . وللقيـــام بـــذلك اتبـــع الخطوات التالية :

أ. من أيقونة **neighborhood Network** الموجدة بسطح المكتـــب ، اضغط بالمفتاح الأيمن للماوس ، فتظهر قائمة ، اختر منهـــا الأمـــر **Properties** .

ب. سوف تظهر نافذة على الشكل التالي :



ج. من القائمة **Network components**، حدد الاختيار **File and print sharing for Microsoft networks** . ثم اضغط مفتاح **File and print sharing**، فتظهر نافذة على الشكل التالي :



د. قم بإزالة التأشير الموجود أمام الاختيـــار الأول والثـــاني ، ثـــم اضـغط مفتاح **Ok** .

4. عندما تستخدم حجرات أو برامج الدردشة ، لا تقبل الحصـــول على أي ملف يحمل الامتداد **EXE** ، لأن هـــذه النوعيـــة مـــن الملفات عادة ما تكون **Trojan** كما أوضحنا في الفصول السابقة .. ويجب ملاحظة أنه عادة ما يقوم المخترق بتغيير اسم ملـــف الــــ **Trojan** ليصـــبح مـــثلا علـــى الشـــكل التـــالي **(MyPicture.jpg.exe)** .

5. إذا كنت تقوم بأعمال هامة داخل شبكة الإنترنت مثل الدخول إلى الحسابات المصرفية أو تحويل الأموال ، فيفضل دائما أن تقـــوم بتخصيص حاسب مستقل لتنفيذ هذه المهام . بمعنى أنه لا يجـــب استخدام هذا الحاسب في حجرات أو برامج الدردشة أو تحميـــل البرامج من شبكة الإنترنت .. بالإضافة إلى أهمية تـــأمين هـــذا الحاسب ببرامج **Firewalls** ، وبرامج **Anti virus** .

6. عند تصفح شبكة الإنترنت لا تقم بعمل **Download** لأي برنامج يحمل الامتداد **EXE** إلا عن طريق المواقع الموثوق بها ، أما إذا كان البرنامج مضغوط على هيئة **ZIP Archive** ، فيمكنك فـــي هذه الحالة تحميل هذه البرامج ، ثم الكشف عنها باستخدام برنامج مضاد للفيروسات .

كلمة أخيره

عند الدخول إلى عالم الـ **Hackers** . هناك عبارة تتردد بكثرة تقول **(you are your systems worst enemy)** أي أنـك العـدو الأول لجهازك .

وهذه حقيقة لا يمكن إنكارها . فمعظم الإحصـاءات تشـير إلـى أن احتمالات عملية الاختراق تكون بنسبة 90% نتيجة خطأ الضـحية ، و 10% فقط تكون نتيجة خطأ في برامج التأمين !!!

إن نسبة قليلة من الـ **Hacker** يقومون باختيـار الضـحية بشـكل عشوائي ، أما معظمهم فيحاولون اجتذاب الضحية والتعرف عليه أولا قبل تنفيذ الاختراق .. إن هذا الأسلوب يمنح المخترق متعه أكبر في اختراق جهاز الضحية ، وهذا أقصى ما يبغيه المخترق ...

إن عالم **Hacking** ليس بالسهولة التي تتصورها .. فالمخترق يحاول دائما اكتساب ثقة الضحية وخداعه قبل التسلل إلى حاسـبه ، وهـذا الخداع يحتاج إلى وقت طويل وتخطيط .. مما يجعل برامج الدردشة الحل السحري للتقرب من الضحية ...

إن عالم **Chat** يجعلك تبوح بكل ما في داخلك دون خوف أو رهبة ، خاصة إذا كان الطرف الآخر مستمع جيد ومتفهم لما تقوله .. إن ذلك يجعلك تثق في هذا الشخص دون أن تراه ، تتخيله من خلال كلماته .

وعندما تصل إلى هذه المرحلة ، تجد أنك ترغب في المزيد .. تريــد أن ترى هذا الشخص الرائع الذي تتحدث إليـــه .. يســألك إذا كنـت ترغب في الحصول على صورته .. وبالطبع توافق !!

ومن هنا تبدأ مرحلة جديدة من الثقة .. إلى أن تصحو يوما لتجد أنك تعيش في عالم من الخيال ...

الإسكندرية في

2004/12/27

المحتويات

لن تنتهى علاقتنا بشرائك للكتب
فسنظل ندعمك بالتمارين والبرامج
والاستشارات المجانية
من خلال موقعنا على الإنترنت
www.egyptbooks.net

تحذير : الكتاب محمى بعلامات مميزة ومسجلة ومن يحاول التزوير يعرض نفسه ومعاونيه للمسا ءلة الجنائية .

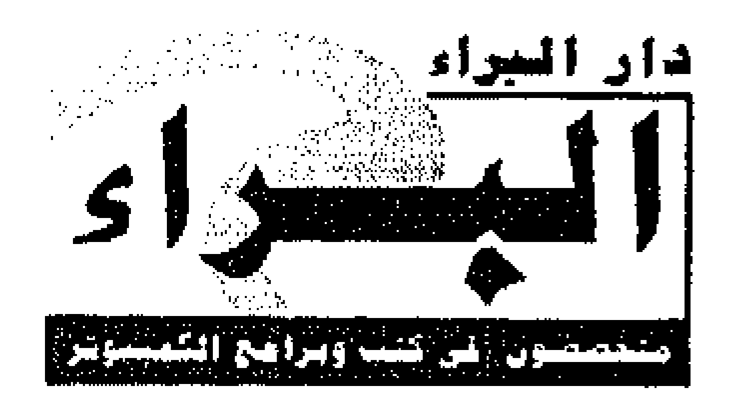
طبعة يناير 2005

رقم الإيداع

2005/1907

ISBN

977-17-1966-1



المركز الرئيسى : 11 شارع د/محمد رأفت – محطة الرمل – الإسكندرية

تليفون وفاكس : 4838326 (03)(2+)

موبايل : 0101634294 (2+) - 0123357844 (2+)

Email : info@egyptbooks.net

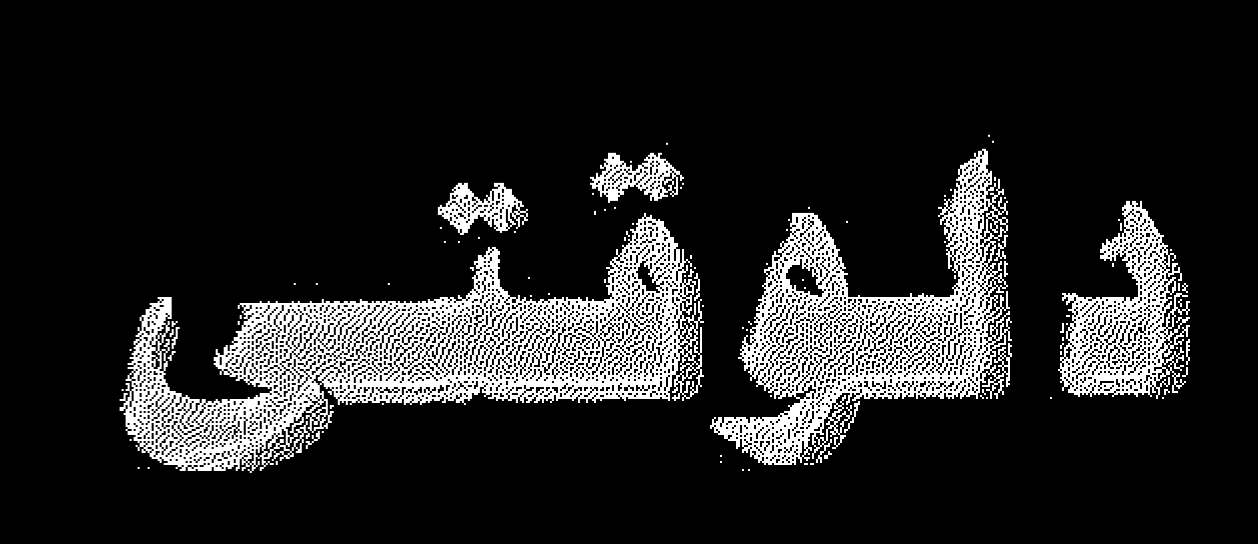
URL: www.egyptbooks.net

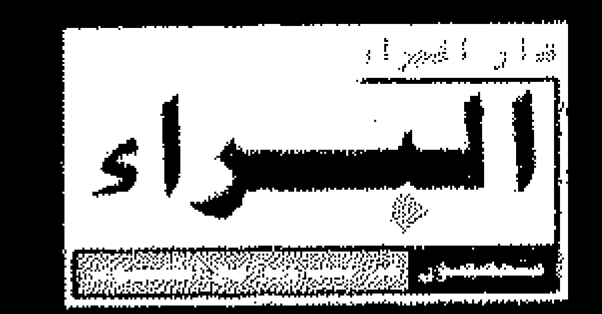
هذا الكتاب ...



والعديد من المهام ...

Bibliotheca Alexandrina
0461899





المركز الرئيسى : ١١ شارع د/محمد رأفت - محطة الرمل - الإسكندرية
تليفون وفاكس : 4838326 (03)(2+)
موبايل : 0101634294 (2+) - 0123357844 (2+)

للدعم الفنى ننتظرك بشبكة الكتب المصرية
www.egyptbooks.net
الموقع الرسمى لدار البراء